KING & SPALDING

King & Spalding LLP
1180 Peachtree Street N.E.
Atlanta, GA 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100
www.kslaw.com

Phyllis B. Sumner
Direct Dial: +1 404 572 4799
psumner@kslaw.com

Application GRANTED.

8/26/2020

LEWIS J. LIMAN
United States District Judge

August 24, 2020

Via ECF

Judge Lewis J. Liman, United States District Judge
United States District Court
Southern District of New York
500 Pearl Street, Room 701
New York, NY 10007
(212) 805-0226

Re: *Culbertson et al. v. Deloitte Consulting LLP*, Case No. 1:20-cv-3962-LJL

Dear Judge Liman:

We represent Defendant, Deloitte Consulting LLP ("Deloitte), in the above-captioned action, and write pursuant to Your Honor's Individual Practice Rule 2.G. and the Standing Order for Electronic Filing Under Seal in Civil and Miscellaneous Cases, 1:19-mc-00583-CM, to respectfully request permission to file a redacted version of Exhibit 1 to the Declaration of Phyllis B. Sumner ("the Sumner Declaration"), and to file an unredacted version of Exhibit 1 under seal, in support of Deloitte's Motion to Dismiss, which is being filed today.

Exhibit 1 to the Sumner Declaration, which is the April 13, 2020 "Contract Between the Ohio Department of Job and Family Services ("ODJFS") and Deloitte Consulting LLP," contains information that ODJFS considers to be confidential.[1] Specifically, the redacted material discusses various security requirements and measures Deloitte and ODJFS agreed to. While it is a non-party, ODJFS has requested that Deloitte redact the information in Exhibit 1 because of its security concerns that the redacted information, if disclosed, would pose a risk to the security of its systems and data. *See* Sumner Declaration at ¶ 2. Under Ohio law, by which ODJFS is governed, security records and infrastructure records, such as those that were redacted here, are exempt from public records. *See, e.g.,* Ohio Rev. Code § 149.433(B)(1) ("A record kept by a

[1] A copy of Exhibit 1, with proposed redactions applied, is submitted as an attachment to this letter-motion. The redactions are located at pages 41-50, 52-66, 68-82, and 88-91.

public office that is a security record is not a public record under section 149.43 of the Revised Code and is not subject to mandatory release or disclosure under that section.").

The presumption that papers filed in connection with a motion are public records can be outweighed by countervailing factors. *See, e.g.*, *Lugosch*, 435 F.3d at 119-120. "'Documents may be sealed if there are on the record findings are made demonstrating that closure is essential to preserve higher values and is narrowly tailored to serve that interest.'" *Id.* at 120 (quoting *Matter of New York Times Co.*, 828 F.2d 110, 116 (2d Cir. 1987)).

Indeed, courts have repeatedly recognized exceptions to the presumption of public access in order to protect the kind of confidential information in Exhibit 1. *See, e.g., Welsh-Huggins v. Ofc. of the Prosecuting Atty., Jefferson Co., Oh.,* 133 N.E.3d 550, 558 (Oh. Ct. App. 2019) (preventing public access to a video of courthouse security and incident response pursuant to the exception provided in Ohio Rev. Code § 149.433); *Encyclopedia Brown Productions. Ltd. v. Home Box Office, Inc.*, 26 F. Supp. 2d 606, 612-613 (S.D.N.Y. 1998) (withholding from disclosure confidential business information that would harm defendants' competitive position); N*ixon v. Warner Communications, Inc.*, 435 U.S. 589, 598 (1978) ("courts have refused to permit their files to serve…as sources of business information that might harm a litigant's competitive standing") (citations omitted); *see also* Fed. R. Civ. P. 26(c)(1)(G) (a court may issue an order "requiring that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specified way.").

Deloitte's, and ODJFS's, interests in protecting the redacted information should outweigh the need for public access because the various security measures and requirements discussed are precisely the type of information that courts protect from public disclosure. Pursuant to Rule 26(c)(1)(G) of the Federal Rules of Civil Procedure, Deloitte respectfully requests that the redacted information in Exhibit 1 to the Sumner Declaration be maintained as redacted from the public record in this matter and that the unredacted version of Exhibit 1 be maintained under seal.

Thank you for Your Honor's attention to this matter.

Respectfully submitted,

/s/ Phyllis B. Sumner
Phyllis B. Sumner

EXHIBIT 1

Redacted per Letter-Motion to Seal

A CONTRACT BETWEEN

THE OHIO DEPARTMENT OF JOB AND FAMILY SERVICES

AND

DELOITTE CONSULTING LLP

THIS CONTRACT is between the State of Ohio Department of Job and Family Services (the "State") and Deloitte Consulting LLP (the "Contractor) and consists of the following:

1. This one-page Contract in its final form;
2. The attached uFACTS PUA/DUA Statement of Work, which incorporates Supplement - A State IT Policy, Standard and Service Requirements; Supplement S - State Information Security and Privacy Requirements, and State Data Handling Requirements; and the JFS -DAS Security Supplement Addendum; and dated April 13, 2020;
3. The Acceptance of uFACTS SOW General Terms and Conditions dated April 13, 2020;
4. The uFACTS PUA/DUA Cloud Services Agreement (CSA) dated April 13, 2020; and
5. The applicable Purchase Order.

Change Orders and amendments issued after the Contract is executed may expressly change the provisions of the Contract. If they do so expressly, then the most recent of them will take precedence over anything else that is part of the Contract.

TO SHOW THEIR AGREEMENT, the parties have executed this Contract as of the dates below.

DELOITTE CONSULTING LLP

By: John B. White

Title: Principal

Date: 4/13/20

STATE OF OHIO

DEPARTMENT OF JOB AND FAMILY SERVICES

Kimberly L. Hall

By: Kimberly L. Hall

Title: JFS Director

Date: April 13, 2020

uFACTS PUA/DUA Statement of Work
April 13, 2020

This Statement of Work is by and between Deloitte Consulting LLP ("Deloitte" or "Deloitte Consulting") and The State of Ohio Department of Job and Family Services (The "State"), effective as of _____, 2020,and is governed by the uFACTS SOW General Terms and Conditions and the uFACTS CSA dated as of [ ], which is incorporated herein by this reference.

Project Approach

Deloitte will implement a cloud-based version of our Unemployment Framework for Automated Claim & Tax Services (uFACTS) solution to meet Pandemic Unemployment Assistance (PUA) requirements of the CARES Act and UI Disaster Unemployment Assistance (DUA) claims. The solution provides the State Pandemic Unemployment Assistance (PUA) functionality necessary to support the CARES act, including processing the additional claims load and making PUA and PFUC payments. The solution also supports any regular DUA declarations, providing the State with a DUA solution.

Functional Overview

uFACTS is designed to let the State define and operate PUA/DUA programs. System administrators can define program parameters for PUA and DUA benefit programs. The administrator enters the proper program parameters (effective dates, eligibility criteria, monetary parameters, etc.) and creates the program. The system creates the new program type and name and creates the necessary flows to allow claimants to apply for and, if eligible, receive benefits.

uFACTS for PUA/DUA meets the following high-level functional requirements:

- The system needs to comply with UIPL 16-20 and its associated attachments. Any out of scope requirements will be subject to a standard change request and approval process.
- PUA/DUA Program Setup - The system allows staff to system administrators the program parameters such as begin date, incident date, declaration date, etc. and to successfully establish the program.
- Initial Screening – the system allows claimants to respond to initial screening questions. These questions determine whether the claimant is most likely a traditional state UI claimant or PUA/DUA claimant. If the claimant is a traditional UI claimant, they are directed to file an initial claim with the existing State UI application. If the claimant is a PUA/DUA claimant, they are directed to the uFACTS Initial Claims functionality.
- Initial Claim - uFACTS for PUA/DUA provides a responsive web framework solution which captures the complete PUA/DUA UI claim process per USDOL UIPL rules and regulations. The initial claims application collects pertinent claimant information (such as IRS withholdings and backdating) upfront, and in detail, to increase the timeliness and accuracy of downstream processes. Claimants are required to create a user id and password for uFACTS for PUA/DUA during the initial claim process. Experion ID proofing will be used for identity proofing to validate the claimant, unless the state and Deloitte mutually agree to an alternate solution for SSA verification.
- The state and Deloitte will work together to develop mechanisms to prevent claimants from being paid from both the regular UI and PUA systems in the same week.

- Monetary Determination - For PUA/DUA claims, uFACTS establishes the PUA/DUA monetary determination based on the earnings information provided by claimant during claim intake process and uses configurable minimum PUA/DUA WBA and maximum PUA/DUA WBA values established during the PUA/DUA Program Setup. Monetaries are recomputed based on revised earnings information.
- Certifications – uFACTS for PUA/DUA provides weekly continued claim certifications functionality. uFACTS displays the questions based on the current program type of the claimant. It can accept the weekly certifications on both personal computers and mobile devices due to its responsive web capabilities.
- Payments - uFACTS for PUA/DUA generates, through the State's payment vendors, payments to eligible PUA/DUA claimants that have completed a weekly certification. The process determines the weekly amount based on the State's rules for PUA/DUA weekly benefit amounts, as well as PFUC. A nightly file is generated to the State's current payment vendor(s) to generate the payment via direct deposit or debit card. Overpayments established within the system can be offset against future payments.
- Adjudication - The main purpose of Adjudication is to help staff determine eligibility for PUA/DUA benefits when issues arise that should potentially prevent payment of benefits. uFACTS has workflow to intelligently route issues to an adjudicator's workflow inbox. This process allows the State to set rules to route the issue to the right adjudicator, using criteria such as the priority of the issue to the business, the skill set of the adjudicator and the timeliness due date of the issue.
- Accounting - The uFACTS for PUA/DUA Fiscal Reporting component tracks all payments made at the claimant level by week, and reports and interface files are generated to allow recording of summary transactions in the State's accounting system.
- Workflow - The uFACTS for PUA/DUA Solution provides workflow functionality through the integrated Business Process Framework powered by IBM Case Foundation.

uFACTS for PUA/DUA

uFACTS for PUA/DUA is a component-based, multi-tiered architecture. The uFACTS Technical Architecture provides the State a system that meets the functional requirements of PUA. Our uFACTS for PUA/DUA Technical Architecture:

1. Is built-on n-tiered, component-based open framework to support the needs of the PUA/DUA processes.
2. Is built on Microsoft .NET programming stack, including ASP.NET and C# for its core application, jQuery JavaScript libraries.
3. Uses pre-configured components whenever possible to reduce development, testing, and implementation time.
4. Adheres to Service-Oriented Architecture (SOA) design principles to reuse business logic, reducing integration complexities.
5. Is a modular solution that eases integration with other components or systems, such as COTS products, federal systems, and other state agencies.
6. Is based on a modern architectural design that provides extensibility and scalability.

7. Is designed with data accuracy and integrity, policy and business logic, and automated workflow and incorporates integrated, intelligent workload management and distribution to help improve business process efficiency.

Technical Architecture uFACTS for PUA

The following graphic depicts the model Cloud deployment of uFACTS for PUA/DUA:

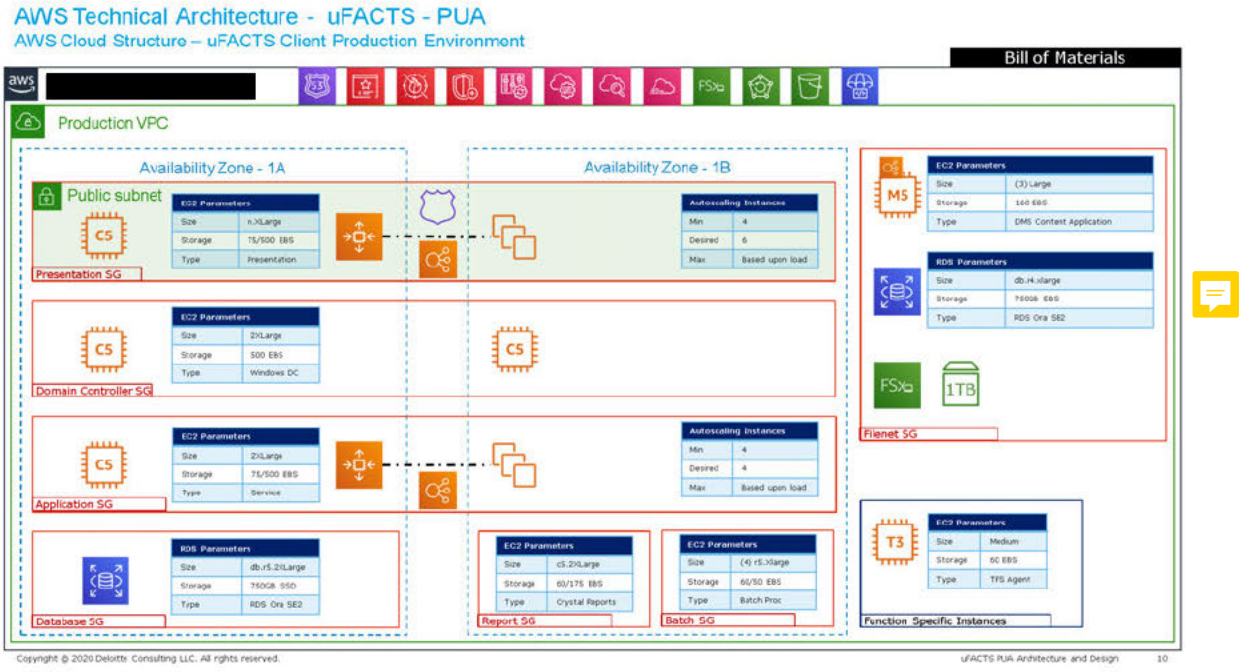


Figure 1: uFACTS Production Environment

uFACTS for PUA/DUA will be hosted on US Regions of Amazon Web Services Commercial Cloud, which operates under multiple security compliance programs, such as CSA, ISO, FedRAMP, FISMA and many others.

User Authentication

uFACTS for PUA/DUA includes OKTA's FedRAMP compliant identity solution for authentication which wraps around uFACTS Microsoft Active Directory for user management and for authorization services for claimant and staff users. OKTA and IOP OHID portal integration (OH|ID) will occur after go live. As detailed requirements unfold, the State and Deloitte will assess project impact and determine and agree to the scope, schedule and an equitable adjustment to the fees using a standard change request and approval process.

Interfaces

With the timely assistance of State business and technical staff, uFACTS for PUA/DUA will incorporate the interfaces below as part of the implementation. These interfaces must be completed and tested in order to place the DUA application in production. Supported interfaces will consist of:

- Scanning and Indexing – for inbound paper documents such as wage verification documents, eligibility verification information, etc. Interfaces will need to be established to the uFACTS Document Management System
- Printing – to generate outbound correspondence to the PUA/DUA claimant
- Payment/Bank Interface – daily outbound payment file to existing bank or payment service (direct deposit or EBT)
- Accounting– outbound interface to the State's financial account system with summary transaction data.
- UI Tax System – A routine (automated and scheduled) interface to uFACTS of all wage information to verify that PUA applicants do not have wage information in the system
- UI Benefits System – A routine (automated and scheduled) interface that provides existing claim information along with the status of the claim including exhausted and ineligible claims. This interface will provide details required to administer the PUA program as defined by DOL in related UIPL(s).
- Child Support Offset – allows for a nightly batch interface to SETS system to allow for offsets. This is a bi-directional interface into and out of SETS.

Cloud Hosting

Deloitte will implement uFACTS for PUA/DUA on a dedicated, state specific account within a commercial Cloud provider and configure and maintain the Cloud environment throughout the project. As part of the scope of this SOW, Deloitte will provide all necessary infrastructure and 3rd-party software required to support the uFACTS solution via this commercial Cloud provider.

In addition, Deloitte will manage the Cloud environment for the application, addressing the following services:

- Cloud and Hosting Services Build and Configure
- Incident and Change Management
- Service Reporting
- Monitoring and Alarming
- Security
- Network Connectivity
- Performance and Capacity Management
- Cost Management
- Backup and Restore
- Operating System Management

Training

Deloitte will conduct the following training service for the State users that will work with uFACTS to service PUA customers: Deloitte will create a training region and training material and deliver training in three training sessions for staff end users 1 week prior to go live. Deloitte will provide the State with all the training materials in an editable format so they may maintain the training post go live. We will also conduct one train the trainer to State training staff within 6 weeks of the PUA go live date. Further details of the training sessions are described below in the Deloitte Responsibilities section.

Claims Processing Capability

As a contemplated option, the State is working with Deloitte regarding the implementation of a uFACTS PUA/DUA claims processing capability to process UI claims from adjudication through settlement. As detailed requirements unfold, the State and Deloitte will assess project impact and determine and agree to the scope, schedule and an equitable adjustment to the fees using a standard change request and approval process.

Transition Services

Deloitte agrees to provide Transition Services to the State, that will, at a minimum:

- Provide assistance, cooperation and information as is reasonably necessary to help enable a smooth transition of the applicable solution and/or services to the State or its designated service provider.
- Transfer State-owned data (detail and summary), information, deliverables, work products, documentation, etc.
- Identify any dependencies on the new service provider necessary for Deloitte to perform the transition services.
- Assist the State in the identification of significant potential risk factors and mitigation strategies relating to the transition.
- Agree to a schedule and plan for Deloitte's return to the State of (i) the State service locations then occupied by Deloitte (if any), and (ii) the State Confidential Information, the State Data, documents, records, files, tapes and disks in Deloitte's possession.

Deloitte agrees to provide transition services during the transition of the solution to DAS OIT and at Project close.

During stabilization of the uFACTS PUA/DUA solution the State and Deloitte agree to transition Deloitte's instance of AWS to the State of Ohio Enterprise brokered public cloud service (AWS) currently hosted by DAS OIT. At the time of this transition, the State and Deloitte will determine if an equitable adjustment to the fees is necessary.

Project Timeline

Deloitte will complete the project in the Three Phases: Adaption and Implementation, Hypercare and Maintenance and Operations (M&O):

- **Adaptation and Implementation** configures uFACTS for PUA/DUA to address the State-specific requirements for user access, monetary calculations, scanning/imaging interface, payment and accounting interfaces, other interfaces, testing and training.
- **Hypercare** is a five-month support and stabilization period. Deloitte is responsible for maintenance and operations of uFACTS PUA/DUA during this period, consisting of application monitoring, defect fixes (including material nonconformities to the product and approved requirements) and ongoing project management. All system enhancements (changes to the approved requirements) will be subject to a standard change request and approval process and incorporated at no additional cost within the capacity of the Hypercare team, approximately 17 FTEs during this period. Deloitte will respond to all Tier 1 (initial State user contact and troubleshooting), Tier 2 (generally application level troubleshooting) and Tier 3 (supporting

component and infrastructure troubleshooting) support tickets, providing support to State users.

- **Maintenance and Operations** is a two-month period of ongoing maintenance and operations support. Team size is reduced and uFACTS for PUA/DUA transition plan is completed. Deloitte is responsible for maintenance and operations of uFACTS PUA/DUA during this period, consisting of application monitoring, defect fixes (material nonconformities to the approved requirements) and ongoing project management. All system enhancements (changes to the approved requirements) will be subject to a standard change request and approval process and incorporated based upon the capacity of the Maintenance and Operations team, approximately 11 FTEs during this period. Deloitte will respond to all Tier 1, Tier 2 and Tier 3 support tickets, providing support to State users.
- Optionally, the State can negotiate Deloitte support beyond the Maintenance and Operation period, in accordance with the standard Amendment, change request and approval process.

The following Gantt chart provides a high-level plan for the Project.

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors
1		**uFACTS for PUA Implementation and Operations**	**189 days?**	**Mon 4/13/2**	**Thu 12/31/2**	
2		**Adaptation and Implementation**	**20 days?**	**Mon 4/13/2**	**Fri 5/8/20**	
3		Project Kick Off	1 day?	Mon 4/13/2	Mon 4/13/2	
4		**uFACTS Installation and Configuration**	**10 days**	**Mon 4/13/2**	**Fri 4/24/20**	
5		Installation of uFACTS for PUA Base Solution	2 days	Mon 4/13/2	Tue 4/14/2(	3SS
6		Milestone 1: uFACTS for PUA Installed	0 days	Tue 4/14/2(	Tue 4/14/2(	5FS-1 day
7		Confirmation of State business rules for PUA - payment calculations, state specific	5 days	Mon 4/13/20	Fri 4/17/20	3SS
8		Development of Interfaces	8 days	Wed 4/15/2	Fri 4/24/20	5
9		uFACTS for PUA Application Configuration	5 days	Mon 4/20/2	Fri 4/24/20	7
10		**Testing**	**13 days**	**Mon 4/20/2**	**Wed 5/6/20**	
11		SIT testing	7 days	Thu 4/23/2(	Fri 5/1/20	9SS+3 days
12		Execute Performance Testing	5 days	Mon 4/27/2	Fri 5/1/20	9
13		Partner Integration Testing	5 days	Mon 4/27/2	Fri 5/1/20	8
14		Development of UAT Test Cases	5 days	Mon 4/20/2	Fri 4/24/20	7
15		UAT Execution	3 days	Mon 5/4/20	Wed 5/6/20	11
16		**Training**	**10 days**	**Mon 4/20/2**	**Fri 5/1/20**	
17		Update of Standard UFACTS for DUA Training	10 days	Mon 4/20/2	Fri 5/1/20	7
18		Deliver End User Training Session 1	1 day	Tue 4/28/2(	Tue 4/28/2(	
19		Deliver End User Training Session 2	1 day	Wed 4/29/2	Wed 4/29/2	
20		Deliver End User Training Session 3	1 day	Thu 4/30/2(	Thu 4/30/2(	
21		**Implementation**	**2 days?**	**Thu 5/7/20**	**Fri 5/8/20**	
22		Final Build	2 days	Thu 5/7/20	Fri 5/8/20	15
23		Go Live	1 day?	Fri 5/8/20	Fri 5/8/20	22FS-1 day
24		Milestone 2: uFACTS for PUA live	0 days	Fri 5/8/20	Fri 5/8/20	23FS-1 day
25		**Hypercare**	**126 days**	**Fri 5/8/20**	**Fri 10/30/2(**	
27		**Maintenance and Operations**	**44 days**	**Mon 11/2/2**	**Thu 12/31/2**	

Figure 2: Draft Project Plan

Deloitte Responsibilities

Deloitte's responsibilities during the Project consist of the following:

Adaption & Implementation Phase:

- Project Management
    - Conduct Weekly Status Meeting with Project Sponsor

    - Conduct daily stand up with Project Manager
- Installation of Base uFACTS for PUA/DUA on Cloud environment.
- Configuration of uFACTS for PUA/DUA based on State-provided, State-specific business rules in areas such as:
    - Initial Triage Questions (Determine Regular UI vs PUA)
    - Monetary calculation
    - Scanning Indexes
    - Correspondence
- Interface development within uFACTS for PUA/DUA environment
- Execute System Integration Testing
- Execute Performance Testing based on estimated load
- Execute Partner Integration Testing
- Perform three pre-implementation training classes for identified State staff that will work with uFACTS for PUA
- Create three online videos for claimants on how to register and utilize the PUA/DUA application. The trainings are:
    - How to Register and Submit Initial Claim
    - How to provide Wage Verification Data
    - How to Submit Weekly Certifications
- Resolve Critical and High application defects identified in UAT
- Deliverables:
    - Installation of base uFACTS for PUA/DUA
    - Configuration Specification Document
    - Configuration and Deployment of uFACTS for PUA/DUA into production
    - Weekly status reports

Hypercare Phase

- Project Management
    - Conduct Weekly Status Meeting with Project Sponsor
- Work to resolve prioritized defects (as defined above) and approved enhancements within team capacity
- Monitor application performance
- Within the capacity of the Hypercare team, appeals will be addressed post implementation
- Deliverables:
    - Weekly status reports

Maintenance and Operations Phase

- Project Management
    - Conduct Monthly Status Meeting with Project Sponsor
- Work to resolve prioritized defects (as defined above)
- Monitor application performance
- Conduct uFACTS for PUA/DUA application transition activities
- Conduct Project Close out activities

- Deliverables:
    - Weekly status reports

State Responsibilities

State responsibilities consist of the following:

Adaption & Implementation Phase:

- Full Time Positions Required
    - State Project Manager – responsible for management of the activities of the State.
    - State Interfaces Lead – responsible for any changes to interfaces on the State side are made per the Schedule. Coordinating PIT testing with partners
    - State Functional Lead – responsible for supplying all State specific PUA rules and design of any required correspondence in standard uFACTS template. Also, leads defect triage sessions
- Additional Part Time Positions Required
    - State Project Sponsor – provide overall sate leadership and serve as a point of escalation
    - Operational Lead – responsible for identifying State staff that will be performing PUA activities within the application and scheduling of training. Also identifies UAT testers and oversees UAT test script creation and execution.
    - Policy Staff – staff with ability to confirm State PUA business rules
    - PUA/DUA Staff – staff identified to perform PUA/DUA activities must attend training.
    - SIT and UAT Testers – staff to test the application
    - Interface developers – to update and test interfaces
- Activities required:
    - Modifications to existing interfaces, if required
    - Coordination of partner testing activities
    - Develop and execute UAT test scripts
    - Develop and generate claimant and staff communications

Hypercare

- Part Time Positions Required
    - State Project Sponsor – provide overall state leadership and serve as a point of escalation
    - State Project Manager – responsible for management of the activities of the State
    - State Interfaces Lead – responsible for any changes to interfaces on the State side are made per the Schedule
    - Policy Staff – staff with ability to confirm State PUA/DUA business rules
    - SIT and UAT Testers – staff to test the application
    - PUA/DUA Staff – perform PUA/DUA operational activities
    -
- Activities required:
    - Develop and generate claimant and staff communications
    - Perform all PUA/DUA operational activities
    - Scanning and Indexing of returned PUA/DUA documentation

Maintenance and Operations

- Part Time Positions Required
    - State Project Sponsor – provide overall state leadership and serve as a point of escalation
    - State Project Manager – responsible for management of the activities of the State.
    - State Interfaces Lead – responsible for any changes to interfaces on the State side are made per the Schedule.
    - Policy Staff – staff with ability to confirm State PUA/DUA business rules
    - SIT and UAT Testers – staff to test the application
    - State IT Staff- participate in project close out and knowledge transfer sessions for PUA/DUA application
    - PUA/DUA Staff – perform PUA/DUA operational activities
- Activities required:
    - Develop and generate claimant and staff communications
    - Perform all PUA/DUA operational activities
    - Scanning and Indexing of returned PUA/DUA documentation
    - Participate in knowledge transfer sessions

Price and Payment Schedule

Price includes all services described herein and cloud hosting and management for 7 months. Payment will be milestone based as follows:

- Adaptation and Implementation
    - $ 700,000 due when base uFACTS PUA/DUA installation complete
    - $ 5,006,000 due upon uFACTS PUA/DUA implementation in production
- Hypercare and Maintenance and Operations
    - $ 3,903,900 ($557,700 per month)

Assumptions

The following assumptions apply to this engagement, and parties acknowledge that departure from these assumptions may affect the outcome and timeliness of the engagement and will require a change order to address the impact on schedule, cost, and scope.

- In light of the COVID-19 crisis and the pressing need to implement PUA, the State and Deloitte Consulting will be required to prioritize speed over non-critical functionality; decisions will be governed by the need to pay eligible recipients and not non-essential or desirable functionality. Customary State standards and rules for reporting, paperwork and process may require suspension to meet the Project timeline. It is assumed that the implementation will commence where the following criteria has been met:
    - Interfaces listed above have been tested and may be executed, with or without reasonable work-arounds
    - State worker user ids have been created
    - End user training has been performed
    - Help desk has been established and trained
- The State acknowledges that it may need to authorize overtime for State staff to support the Project and State responsibilities.

- The State will dedicate or obtain the staffing resources necessary to support the timely execution of this critical project in accordance with the necessary aggressive project schedule.
- Deloitte Consulting will implement the base uFACTS for PUA/DUA solution; customizations to Deloitte Consulting's solution and other changes, including, without limitation, any due to new Federal guidelines or State requirements, will require a mutually executed change order given the need for additional resources and the impact of such changes on the project schedule and pricing.
- The State will be responsible for aligning all 3rd party vendors and systems that are required to interface with the new PUA system (i.e., payment systems, banks, EBT providers, State accounting systems), coordinating the timely execution of any agreements, the coordination of testing and the collaboration of participating partners. Deloitte will collaborate with the State and 3rd party vendors in finalizing these interfaces for production, using existing interface specifications.
- Current State technical documentation exists for each interface listed above and that it can rely on such documentation in development of those interfaces.
- The State and its payment providers can accept payment and financial reporting files and agrees to process payment files generated by the system, according to the interface standard.
- The State will work with existing State UI bank or payment service to ensure they can receive and process PUA/DUA payment file separate from State regular UI Payment file, according to the interface standard. The interfaces generated by uFACTS will contain PUA data only.
- The recent compromised performance of Federal integrity checks may require that such integrity checks be suspended to ease the customer experience. Integrity may have to be enforced by the State on the back end, or through subsequent releases of cross-match or other integrity capabilities.
- Offsets to collect amount due balances from other programs (e.g. UI) are not within the scope of this agreement. If desired, automated interfaces may be considered to be built and deployed post-implementation, subject to the capacity of the Hypercare team.
- Offsets for child support may be implemented as a secondary release and must be accommodated within the capacity of the Hypercare team.
- There will be no interface from uFACTS for PUA/DUA to ICON Services.
- The PUA System will include integration with Experion identity services. Failure to authenticate with the Experion services shall permit or withhold payment, as per the State's choice, and create an identity adjudication issue within the system that staff may elect to respond to.
- Users will authenticate with uFACTS built-in Active Directory Services, unless integration with an enterprise IAM tool can be accomplished during the project timeline. Users will receive unique login for uFACTS.
- Any interfaces other than those listed herein will be deferred to a post-implementation release, and subject to Project Change Control processes.
- Due to the nature of social distancing requirements during the COVID-19 crisis, Deloitte staff will work remotely until mutually agreed otherwise, and State staff will interact with the project team using remote videoconferencing. Deloitte staff will be provided promptly with any access credentials needed to complete the services.
- Development and implementation activities, such as coding and testing, may be conducted by staff located offshore as well as onshore. No state data will be stored offshore and unobfuscated production data shall not be viewed or accessed by offshore resources.

- There will be no data conversion included prior to implementation. The system will only serve new PUA/DUA claimants. Any back conversion of data is subject to inclusion in the Hypercare capacity.
- The processing capacity included in this SOW is based on an assumption of the AWS Production Environment in Figure 1: uFACTS Production Environment. Should increased Cloud computing power and capacity be required due to claimant volume, the parties will process an appropriate change order to this SOW to adjust such capacity and associated Cloud hosting fees.
- The State and Deloitte agree to participate in Project Health Check Meeting(s), as deemed necessary.

Supplement A:

State IT Policy, Standard and Service Requirements

Revision History:

Date:	Description of Change:
1/01/2019	Original Version
10/18/2019	Updated to modify service descriptions, include new services, and remove older services. A new Appendix A - Request for Variance to State IT Policy, Standard or Service Requirements was added.

Contents

1. Overview of Supplement 4

2. State IT Policy and Standard Requirements ..... Error! Bookmark not defined.

3. State IT Service Requirements 5

3.1. Requirements Overview 5

3.2. Solution Architecture Requirements 5

3.3. State of Ohio IT Services 6

3.3.1. InnovateOhio Platform 6

3.3.1.1. Digital Identity Products 6

3.3.1.2. User Experience Products 7

3.3.1.3. Analytics and Data Sharing Products 7

3.3.2. Application Services 8

3.3.2.1. Enterprise Document Management Solution (DMS): 8

3.3.2.2. Electronic Data Interchange (EDI) Application Integration: 8

3.3.2.3. Enterprise Business Intelligence (BI): 9

3.3.2.4. Enterprise eLicense: 9

3.3.2.5. ePayment Business Solution: 10

3.3.2.6. Enterprise eSignature Service: 10

3.3.2.7. IT Service Management Tool (ServiceNow): 11

3.3.2.8. Ohio Benefits: 11

3.3.2.9. Ohio Business Gateway (OBG): 12

3.3.2.10. Ohio Administrative Knowledge System (OAKS): 12

3.3.2.11. Enterprise Geocoding Services (EGS): 13

3.3.2.12. Geographic Information Systems (GIS) Hosting: 13

3.3.3. Data Center Services 13

3.3.3.1. Advanced Interactive eXecutive (AIX): 13

3.3.3.2. Backup: 13

3.3.3.3. Data Center Co-Location: 13

3.3.3.4. Data Storage: 14

3.3.3.5. Distributed Systems DRaaS: 14

3.3.3.6. Mainframe Business Continuity and Disaster Recovery: 14

3.3.3.7. Mainframe Systems: 15

3.3.3.8. Metro Site Facility: 15

3.3.3.9. Server Virtualization: 15

3.3.4. Hosted Services 16

3.3.4.1. Database as a Service: 16

3.3.4.2. Database Support: 16

3.3.5. IT Security Services 17

3.3.5.1. Secure Sockets Layer (SSL) Digital Certificate Provisioning: 17

3.3.6. IT Support Services 17

3.3.6.1. Enterprise End User Support: 17

3.3.6.2. Enterprise Virtual Desktop: 17

3.3.7. Messaging Services 18

3.3.7.1. Microsoft License Administration (Office 365): 18

3.3.8. Network Services 18
3.3.8.1. Ohio One Network: 18
3.3.8.2. Secure Authentication: 19
3.3.8.3. Wireless as a Service: 19
3.3.9. Telephony Services 19
3.3.9.1. Voice Services – VoIP 19
3.3.9.2. Toll-Free Services: 19
3.3.9.3. Automatic Caller Navigation and Contact Center Services (ACD/Contact) Centers: 19
3.3.9.4. Call Recording Services: 20
3.3.9.5. Conferencing 20
3.3.9.6. Fax2Mail: 20
3.3.9.7. Session Initiation Protocol (SIP) Call Paths: 20
3.3.9.8. Site Survivability: 20
3.3.9.9. VoIP related Professional Services and Training: 20
Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements 22

1. Overview of Supplement

This supplement shall apply to any and all work, services, locations and computing elements that the Contractor will perform, provide, occupy or utilize in conjunction with the delivery of work to the State and any access to State resources in conjunction with delivery of work.

This includes, but is not limited to:

- Major and minor projects, upgrades, updates, fixes, patches and other software and systems inclusive of all State elements or elements under the Contractor's responsibility utilized by the State;
- Any systems development, integration, operations and maintenance activities performed by the Contractor;
- Any authorized change orders, change requests, statements of work, extensions or amendments to this contract;
- Contractor locations, equipment and personnel that access State systems, networks or data directly or indirectly; and
- Any Contractor personnel, or sub-contracted personnel that have access to State Data as defined below:
    - "State Data" includes all data and information created by, created for, or related to the activities of the State and any information from, to, or related to all persons that conduct business or personal activities with the State, including, but not limited to Sensitive Data.
    - "Sensitive Data" is any type of data that presents a high or moderate degree of risk if released, disclosed, modified or deleted without authorization. Sensitive Data includes but is not limited to:
        - Certain types of personally identifiable information (PII) that is also sensitive, such as medical information, social security numbers, and financial account numbers.
        - Federal Tax Information (FTI) under IRS Special Publication 1075.
        - Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA).
        - Criminal Justice Information (CJI) under Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy.
    - The data may also be other types of information not associated with an individual such as security and infrastructure records, trade secrets, and business bank account information.
- The terms in this supplement are in addition to the Contract terms and conditions. In the event of a conflict for whatever reason, the highest standard contained in the Contract shall prevail.

Please note that any proposed variances to the requirements outlined in this supplement are required to be identified in Appendix A - Request for Variance to State IT Policy, Standard or Service Requirements. Offerors are asked not to make any changes to the language contained within this supplement. In the event the Offeror finds it necessary to deviate from any of the standards or State IT services, a variance may be requested, and the Offeror must provide a sufficient business justification for the variance request. In the event that a variance is requested post award, e.g., a material change to the architecture, the Enterprise IT Architecture Team will engage with the Contractor and appropriate State stakeholders to review and approve/deny the variance request.

Deloitte has a long history of innovation and a demonstrated ability to execute. We have vast experience in implementing large scale systems transformation for commercial and public sector clients. We have a dedicated and experienced market leading security practice well versed in implementing security controls for the proposed solution. Further, our familiarity with the State's IT architecture, its policies, and its people gives us the insight and experience

necessary to successfully implement the new system to address the State's requirements. Our track record of success equates to significantly reduced risk for our clients.

Deloitte approaches security in a holistic, defense-in-depth manner by incorporating security at each phase of our system development lifecycle – from planning and requirements validation through the migration and into security and vulnerability testing process. We will work with the State to increase the security posture of a security control beyond the current level if desired by leveraging an efficient and transparent change control process to manage those requests.

The Contractor will comply with State of Ohio IT policies and standards. For the purposes of convenience, a compendium of IT policy and standard links is provided in the table below.

Table 1 – State of Ohio IT Policies, Standards, IT Bulletins and DAS Polices

Item	Link
State of Ohio IT Policies	https://das.ohio.gov/Divisions/Information-Technology/State-of-Ohio-IT-Policies
State of Ohio IT Standards	https://das.ohio.gov/Divisions/Information-Technology/State-of-Ohio-IT-Standards
State of Ohio IT Bulletins	https://das.ohio.gov/Divisions/Information-Technology/State-of-Ohio-IT-Bulletins
DAS Policies	100-11 Protecting Privacy 100-12 ID Badges & Visitors Policy 700-00– Technology / Computer Usage Series 2000-00 – IT Operations and Management Series https://das.ohio.gov/Divisions/Administrative-Support/Employees-Services/DAS-Policies

Deloitte understands the IT Policies and Standards of the State as stated above. For implementation of any standards if State desires for the proposed solution to adhere to We will work with the State to increase the security posture of a security control beyond the current level if desire by leveraging an efficient and transparent change control process to manage those requests.

2. State IT Service Requirements

2.1. Requirements Overview

Contractors performing the work under the Contract are required to comply with the standards and leverage State IT services outlined in this document unless the State has approved a variance. See note above in Section 1 regarding instructions to propose variances to the requirements outlined in this supplement.

2.2. Solution Architecture Requirements

Unless stipulated otherwise in the RFP, on premise or cloud-based solutions are permitted by the State. Custom or unique built solutions must comply with State requirements including using the State's virtualized computing platform (State Private Cloud) or the State of Ohio Enterprise brokered public cloud service and running on databases that comply with the State's supported database platforms. Custom or unique built solutions are required to include installation of third-party applications on State provided computing platforms which could be on the State-run private cloud or the State-run public cloud. Dedicated server platforms are not compliant with the State's virtualization requirements. The State provides different storage pools (tiers) of storage with the ability to use and allocate the appropriate storage type based on predetermined business criticality and requirements. Storage pools are designed to support different I/O workloads. Custom or unique built solutions must take advantage of the State's storage service offerings.

Custom or unique built solutions must be developed in open or industry standard languages (e.g. Java, .NET, PHP, etc.). Applications must be developed with standards-based open application programming interfaces and all available features and functionality accessible via APIs must be disclosed in the proposed solution. Custom or unique built solutions with Open APIs proposed must include periodic updates throughout the project lifecycle and a final update as part of the closure phase.

Cloud-based solutions must utilize as many platform services as possible and comply with State requirements to run in the State of Ohio Enterprise brokered public cloud service. Currently, Microsoft Azure and Amazon Web Services are hosted by DAS OIT for the State of Ohio.

2.3. State of Ohio IT Services

The Department of Administrative Services Office of Information Technology (DAS OIT) delivers information technology (IT) and telecommunication services. DAS OIT is responsible for operating and maintaining IT and telecommunication hardware devices, as well as the related software. This document outlines a range of service offerings from DAS OIT that enhance performance capacity and improve operational efficiency. Explanations of each service are provided and are grouped according to the following solution categories.

2.3.1. InnovateOhio Platform

Executive Order 2019-15D, “Modernizing Information Technology Systems in State Agencies,” established the InnovateOhio Platform (IOP) initiative. IOP focuses on digital identity, the experience of the individual authorized to access the system (“User”), analytics and data sharing capabilities. The InnovateOhio Platform provides integrated and scalable capabilities that better serve Ohioans.

2.3.1.1. Digital Identity Products

OH | ID - Digital identity solution for Ohio citizens:
Provides single sign-on for disparate systems, enhanced security and privacy, federal and state compliance, and personalized experience. Simple, secure access for citizens. Multiple levels of identity assurance.

- Single Sign-On
- Access Logging
- Real-Time Analytics
- 2-Factor Authentication (2FA)
- Access Management
- Self-Service Portal
- Identity Proofing
- Directory Integration

OH | ID Workforce - Digital identity solution for Ohio workforce
Provides single sign-on for disparate systems, enhanced security and privacy, federal and state compliance, and personalized experience. Simple, secure access for state and county employees, contractors, and external workers. Multiple levels of identity assurance.

- Single Sign-On
- Directory Integration
- Real-Time Analytics
- 2-Factor Authentication (2FA)
- Just-in-Time Provisioning
- User Management
- Access Logging
- Privileged Access Management

ID Platform – Software as a Service (SaaS) identity framework
Provides an authorization layer and allows for the integration and extension of InnovateOhio Platform identity services into applications. Customizable to User needs.

- Fine-Grain Authorization Management
- Real-Time Analytics
- Extendable Services from OH|ID
- Cloud-Based Infrastructure

2.3.1.2. User Experience Products

IOP Portal Builder - Website template accelerator:
An accelerator to easily create modern, responsive and ADA-compliant websites and portals for the InnovateOhio cloud platform. The InnovateOhio Portal Builder is available in a Software as a Service (SaaS) form.

- Standardized Dynamic Templates
- Automated Workflows
- Governance & Access Control
- Optimized Content Search
- ADA-Compliant
- Content Management
- Integration with OH|ID
- Real-Time Analytics
- Aggregate Applications
- Customizable Features
- Mobile Ready
- Site Analytics

IOP myOhio - The State's Intranet platform
Features intuitive navigation, simplified access to on-boarded business applications, and a modernized, mobile-responsive design. Automates compliance with accessibility standards per Section 508 of the Rehabilitation Act.

- Single Sign-On
- Personalized Content
- Content Management
- Near Real-Time Syndication
- 2-Factor Authentication (2FA)
- Access Logging
- Optimized Content Search
- Application Store
- Mobile Ready
- Automated Workflows
- Real-Time Analytics
- Site Analytics

IOP Digital Toolkit - Free User experience digital toolkit
Reusable components for quick deployment of websites, portals and applications. Universal framework for developers and designers. Consistent and compliant User experiences.

- Mobile Ready
- Real-Time Analytics
- Style Guide
- Customizable Features
- Sample Code
- ADA-Compliant
- Standardized Dynamic Templates

2.3.1.3. Analytics and Data Sharing Products

Applied Analytics
Ohio's applied analytics solution provides the ability to build analytical and reporting solutions and deploy them in the most impactful manner possible by putting data in the hands of Users in their natural workflow. From ideation and solution design to data science and engineering, the applied analytics solution enables the User to move from concept to results.

- Advanced Data Science
- Data Strategy Optimization
- Ideation & Scoping
- Solution Design
- Visual Data Discovery
- Workflow Integration

Big Data Platform
Ohio's data sharing and analytics platform provides public/private cloud deployment models that are secure, flexible, and scalable, powering analytics across data of any type or source to gain deeper insights and drive impactful outcomes.

- Data Sharing
- Diverse Data
- Hybrid Cloud
- Massive Volumes
- Rapid Prototyping
- Real-Time Analytics
- Security & Compliance

Data Management

Ohio's self-service data management suite provides rich and secure capabilities to harness the power of the analytics platform leveraging User friendly and pre-configured technologies. Additionally, the suite supports a bring-your-own-tool approach allowing analysts and data scientists to work on the platform with the technologies they are most comfortable using.

- Audit
- Bring Your Own Tool (BYOT)
- Data Engineering
- Data Exploration
- Data Lineage
- Data Profiling
- Governance & Security
- Pre-Built Pipelines
- Self-Service Support

Please explain how the InnovateOhio Platform will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

Deloitte is the InnovateOhio Platform Managed Services provider to the State. Deloitte provides support for the different InnovateOhio Platform products such as OH|ID, OH|ID Workforce, ID Platform, myOhio, Digital Toolkit. Deloitte has been an advocate of InnovateOhio Platform products to large State agencies such as ODJFS, ODOT, BWC, ODH, OPD, ODM for their digital transformation, user experience, identity and access management needs for their mission critical applications.

Deloitte plans to incorporate InnovateOhio Platform products in future enhancements to the proposed solution by leveraging an efficient and transparent project change control process

2.3.2. Application Services

2.3.2.1. Enterprise Document Management Solution (DMS):

The Enterprise Document Management Solution (DMS) is a standardized, integrated solution for document and content management. The core components of the solution include:

- **Document Management** core capabilities such as: secure check-in / check-out, version control, and index services for business documents, audio / video files, and Environmental Systems Research Institute (ESRI) / Geographic Information Systems (GIS) maps.
- **Image Processing** for capturing, transforming and managing images of paper documents via scanning and / or intelligent character recognition technologies such as Optical Character Recognition.
- **Workflow / Business Process Management (BPM)** for supporting business processes, routing content, assigning work tasks and creating audit trails.
- **Records Management** for long-term retention of content through automation and policy, ensuring legal, regulatory and industry compliance.
- **Web Content Management (WCM)** for controlling content including content creation functions, such as templating, workflow and change management and content deployment functions that deliver content to Web servers.
- **Extended Components** can include one or more of the following: Digital Asset Management (DAM), Document Composition, eForms, search, content and analytics, e-mail and information archiving.

2.3.2.2. Electronic Data Interchange (EDI) Application Integration:

EDI Application Integration service is a combination of Application Integration, Data Exchange and Electronic Data Interchange (EDI) functionality. This service provides application to application connectivity to support interoperable communication, data transformation, and business process orchestration amongst applications on the same or different computing platforms. Business process orchestration between many data formats may be

supported including Web Services, XML, People-Soft, FTP, HTTP, MSMQ, SQL, Oracle, Flat File, SAP, DB2, CICS, EDI, HIPAA, HL7, Rosetta Net, etc.

The Data Exchange component allows unattended delivery of any electronic data format via encrypted files over public FTP, FTPS, SFTP, VPN. Application Integration services are offered via:

- **End Points** – also referred to as a mailbox, this is a connectivity point to facilitate the movement or transaction of data between two or more entities.
- **KBs** – represents the size in kilobytes of a message that is transformed or processed. This typically refers to a document or file conversion or a format change.
- **Messages** – a discrete unit of data that is moved or transacted between two or more entities. A message typically represents a business document or a file.

2.3.2.3. Enterprise Business Intelligence (BI):

The State of Ohio Enterprise Business Intelligence (BI) service provides enterprise data warehousing, business and predictive analytics, and decision support solutions. By turning raw data into usable information, BI helps Users analyze policies and programs, evaluate operations, and drive decisions. The core information available for analysis includes:

Health and Human Services Information

- Ohio Benefits
- Medicaid Claims
- Medicaid Enrollment
- Medicaid Financial
- Medicaid Provider
- Long Term Care
- Medicare Claims
- Pharmacy

Financial Information

- General Ledger
- Travel and Expense
- Procure to Pay
- Capital Improvements
- Accounts Receivable
- Asset Management
- Budget/Planning
- Value Management
- Statewide Cost Allocation Plan
- Minority Business Enterprise (MBE) Program/Encouraging Diversity, Growth and Equity (EDGE) Program

Workforce and Human Resources

- Workforce Profile
- Compensation
- State of Ohio Payroll Projection Systems
- ePerformance
- Enterprise Learning Management

2.3.2.4. Enterprise eLicense:

Enterprise eLicense is the State of Ohio's online system used to manage the issuance, certifications, inspections, renewals and administration of professional licenses across the State. The eLicense application is a public/business facing system that is designed to foster the creation and growth of businesses in the State. The system is a central repository for license and certificate data, in addition to managing the generation and storage of correspondence. Secure fee collection is performed through an on-line payment processor, which includes bank transfers, credit cards, and other payment types. Core system capabilities include:

Customer Relationship Manager (CRM)
- Contact Management

Revenue
- Deposit Accounting Revenue Tracking
- Refund and Reimbursement Processing
- Fine and Penalty Tracking

License Administration
- Administration
- Workflow
- Reports

Enforcement
- Enforcement Activities
- Case Management Activities

Online Licensure Services
- Applications
- Renewals
- License Verification
- License Maintenance
- License Lookup Website
- Workflow
- Document Management
- Secure Payment Processing

Other Services
- Continuing Education Tracking
- Examinations
- Inspections
- Complaint Management

2.3.2.5. ePayment Business Solution:

The CBOSS ePayment Gateway solution is a highly flexible payment engine supporting a wide range of payment types: credit cards, debit cards, electronic checks, as well as recurring, remote capture and cash payments. The CBOSS ePayment Gateway solution utilizes a single, common gateway to permit the acceptance of payments from multiple client application sources: Web, IVR, kiosk, POS, mobile, over the counter, etc. Payment processing is supported through multiple credit card gateway options, automated clearing house (ACH) bank processing, and Telecheck services.

The CBOSS ePayment Gateway solution is compliant with the Payment Card Industry Data Security Standard (PCI DSS), the Electronic Fund Transfer Act (EFTA) and is audited to the standards of SSAE16 SOC1 Type II.

2.3.2.6. Enterprise eSignature Service:

OneSpan Sign is Ohio's enterprise solution for eSignatures. The product is a FedRAMP SaaS (Software as a Service) solution, which offers a standardized approach to cloud security. OneSpan Sign's eSignature functions include workflows, tracking, audit logs and protection against forgery/non-repudiation.

OneSpan Sign has an extensive library of open application programming interfaces (APIs) to integrate eSignatures with existing applications and core systems. OneSpan Sign's pre-built, third-party connectors enable the eSignature capabilities into business software products such as Dynamics CRM, Salesforce, Microsoft SharePoint, etc.

2.3.2.7. IT Service Management Tool (ServiceNow):

DAS OIT offers ServiceNow, a cloud-based IT Service Management Tool that provides internal and external support through an automated service desk workflow-based application which provides flexibility and ease-of-use. ServiceNow provides workflows aligning with Information Technology Infrastructure Library (ITIL) processes such as incident management, request fulfillment, problem management, change management and service catalog. These processes allow for the management of related fields, approvals, escalations, notifications and reporting needs.

Standard ServiceNowFeatures Include:

- **Incident Management** - Manage service disruptions and restore normal operation quickly.
- **Problem Management** - Identify the underlying cause of recurring incidents.
- **Change Management** - Minimize the impact of service maintenance.
- **Configuration Management** - Define and maintain a configuration management database (CMDB) for IT infrastructure.
- **Asset Management** - Manage assets and inventory records.
- **Service Catalog Management** – Automated process for goods and service requests.
- **Knowledge Management** - Gather, store and share knowledge within the organization.
- **Reporting** – Custom reporting.
- **Integration to AD, Event Monitoring, Discovery Tools, Exchange** – Integration to AD, Event Monitoring, Discovery Tools, Exchange – Integration with third-party applications.
- **Customized Portal Pages** – User friendly interface to create engaging and robust portals, dashboards, and applications.
- **Software Asset Management** – End to end software life cycle management on a single platform, to optimize spend and reduce compliance risk.
- **IT Operations Management (ITOM)** - Includes event management, service mapping, discovery, orchestration and cloud management.

2.3.2.8. Ohio Benefits:

Ohio Benefits provides a comprehensive and effective platform for planning, designing, development, deployment, hosting and ongoing maintenance of all State of Ohio Health and Human Services (HHS) Public Assistance Services and Programs.

Ohio Benefits provides superior eligibility services including citizen self-service, efficient workflow management and coordination, an agile and easily manageable rules engine, improved data quality and decision support capabilities. Ohio Benefits supports improvement in State and county productivity, capability and accessibility of benefits to Ohioans through a robust enterprise system. The Ohio Benefits platform provides four distinct technology domains:

1. **Common Enterprise Portal** – User Interface and User Experience Management, Access Control, Collaboration, Communications and Document Search capability.
2. **Enterprise Information Exchange** – Discovery Services (Application and Data Integration, Master Data Management (MDM), Master Person Index and Record Locator Service), Business Process Management, Consent Management, Master Provider Index and Security Management.

3. **Analytics and Business Intelligence** – Integration and delivery of analytics in the form of alerts, notifications and reports.
4. **Integrated Eligibility** – A common Enterprise Application framework and Rules Engine to determine eligibility and benefits for Ohio Public Benefit Programs.

Privacy and security are the foundational blocks of the platform which is compliant with all State and federal standards.

2.3.2.9. Ohio Business Gateway (OBG):

The Ohio Business Gateway (OBG) offers Ohio's businesses a time and money saving online filing and payment system that simplifies business' relationships with government. Ohio businesses can use OBG to access various services and electronically submit transactions and payments. The OBG also offers the ability for business to view historical filings (and payments) and allows for business activities to be provided by a third-party provider of professional accounting services. OBG Electronic Filing also partners with local governments to enable businesses to file and pay selected Ohio municipal income taxes.

OBG Electronic Filing routes data and payment information directly to program administrators so that they may continue to manage the overall account relationship.

2.3.2.10. Ohio Administrative Knowledge System (OAKS):

The Ohio Administrative Knowledge System (OAKS) is the State's Enterprise Resource Planning (ERP) system which provides central administrative business services such as Financial Management, Human Capital Management, Content Management, Enterprise Learning Management and Customer Relationship Management. Core system capabilities include:

Content Management (myohio.gov)
- Centralized Communications to State Employees and State Contractors
- OAKS alerts, job aids and news
- Statewide News
- Password Reset for Active Directory

Customer Relationship Management (CRM)
- Contact / Call Center Management

Enterprise Business Intelligence
- Key Financial and Human Resources Data, Trends and Analysis
- Cognos driven reporting
- Targeted Business Intelligence
- Tableau Analytics and Visualization

Enterprise Learning Management (ELM)
- Training Curriculum Development
- Training Content Delivery
- Training Status Tracking and Reporting

Financial Management (FIN)
- Accounts Payable
- Accounts Receivable
- Asset Management
- Billing
- eSourcing
- Financial Reporting
- General Ledger

- Planning and Budgeting
- Procurement
- Travel & Expense

Human Capital Management (HCM)

- Benefits Administration
- eBenefits
- ePerformance
- Kronos
- Payroll
- Position Management
- Time and Labor
- Workforce Administration

2.3.2.11. Enterprise Geocoding Services (EGS):

Enterprise Geocoding Services (EGS) combine address standardization, geocoding, and spatial analysis into a single service. Individual addresses can be processed in real time for online applications or large numbers of addresses can be processed in batch mode.

2.3.2.12. Geographic Information Systems (GIS) Hosting:

GIS Hosting delivers dynamic maps, spatial content, and spatial analysis via the Internet. Users can integrate enterprise-level GIS with map capabilities and spatial content into new or existing websites and applications.

Please explain how the State's Application Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

Deloitte will leverage the State's published IT Application Services.

2.3.3. Data Center Services

2.3.3.1. Advanced Interactive eXecutive (AIX):

AIX is a proprietary version of the UNIX operating system developed by IBM. DAS OIT runs the AIX operating system on IBM Power hardware, as a physical server or logical partition (LPAR)/virtual server. All of the AIX systems are connected to the DAS OIT Enterprise Storage Area Network (SAN) for performance, general purpose or capacity-based storage. All systems are also provided backup and recovery services.

2.3.3.2. Backup:

The Backup service uses IBM Tivoli Storage Manager Software and provides for nightly backups of data. It also provides for necessary restores due to data loss or corruption. The option of performing additional backups, archiving, restoring or retrieving functions is available. DAS OIT backup facilities provide a high degree of stability and recoverability as backups are duplicated to the alternate site.

2.3.3.3. Data Center Co-Location:

The DAS OIT Co-Location service offers a Tier 3 capable secure data center environment with reliable uptime, power redundancy and redundant cooling to ensure uninterrupted access of critical data and applications in the State of Ohio Computer Center (SOCC). The SOCC is staffed and available to authorized personnel 24x7x365 and is accessible via electronic card key only.

2.3.3.4. Data Storage:

The services covered under Data Storage include:

High Performance Disk Storage service offers high-performance, high-capacity, secure storage designed to deliver the highest levels of performance, flexibility, scalability and resiliency. The service has fully redundant storage subsystems, with greater than five-nines availability, supporting mission critical, externally-facing and revenue-generating applications 24x7x365. High Performance Disk Storage is supplied as dual Enterprise SAN fiber attached block storage.

General Purpose Disk Storage service offers a lower-cost storage subsystem, which is not on a high performance disk. This service supports a wide range of applications, including email, databases and file systems. General Purpose Disk is also flexible and scalable and highly available. General Purpose Disk Storage is supplied as dual Enterprise SAN fiber attached block storage.

Capacity Disk Storage service is the least expensive level of disk storage available from DAS OIT. Capacity Disk is suitable for large capacity, low performance data, such as test, development and archival. Capacity Disk Storage is supplied as dual Enterprise SAN fiber attached block storage or as file-based storage.

2.3.3.5. Distributed Systems DRaaS:

Distributed Systems Disaster Recovery as a Service (DRaaS) offers server imaging and storage at a geographically disparate site from Columbus. The service provides a private Disaster Recovery as a Service solution connected to the State of Ohio Computer Center (SOCC) via the Ohio One Network that will consists of the following:

- Compute to allow expected performance in the event of a complete failover
- 24vCPU per host with 32 host in the environment all licensed with VMWare
- Support of the orchestration and replication environment
- Site connectivity
- Stored images available upon demand

Open Systems Disaster Recovery - Windows (1330 / 100607 / DAS505170/ 3854L) - Open Systems Disaster Recovery – Windows is a service that provides a secondary failover site for Windows based servers within the geographically disparate site. This service provides duplicative server compute and storage to match Server Virtualization and Data Storage capabilities as provisioned at the SOCC. This service is provided through a contracted third party who is responsible for all management and equipment at the facility.

Open Systems Disaster Recovery - AIX (1330 / 100607 / DAS505170/ 3854N) - Open Systems Disaster Recovery – AIX is a service that provides a secondary failover site for AIX based servers within the geographically disparate site. This service provides duplicative server compute and storage to match AIX Systems Services and Data Storage capabilities as provisioned at the SOCC. This service is provided through a contracted third party who is responsible for all management and equipment at the facility.

2.3.3.6. Mainframe Business Continuity and Disaster Recovery:

Business continuity involves planning for keeping all aspects of a business functioning in the midst of disruptive events. Disaster recovery, a subset of business continuity focuses on restoring the information technology systems that support the business functions.

Mainframe Disaster Recovery (DR) services are available for DAS OIT's IBM mainframe environment. Services are made available via IBM's Business Continuity and Resiliency Services, which provides hot site computer facilities at a remote location.

Tests are conducted bi-annually at IBM's hot site location, during which DAS OIT's mainframe computer infrastructure is restored. Once the mainframe system is operational, production applications are restored and extensive tests are conducted to ensure that those applications have been successfully recovered and would be available in the event of an actual disaster.

This service is designed to expand business continuity and disaster recovery capabilities in the most cost effective and efficient manner possible.

2.3.3.7. Mainframe Systems:

DAS OIT's Mainframe Systems services offer an IBM mainframe computer sysplex with a processing speed rating at 5,700 Million of Instructions per Second (MIPS). This mainframe uses the z/OS operating system and the Job Entry Subsystem (JES3). Additionally, the system is connected via fiber to DAS OIT's High Performance Disk Storage, which affords reliable and fast disk access and additional storage capacity when needed.

Services are provided using a wide range of application, transaction processing and telecommunications software. Data security and User authentication are provided by security software packages. Mainframe tape service option is available:

- Mainframe Virtual Tape - Virtual tape technology that optimizes batch processing and allows for better tape utilization using the EMC Disk Library for Mainframe (DLM) virtual tape.

2.3.3.8. Metro Site Facility:

The Metro Site Facility Service provides a secondary, near real-time (measured in ms) failover from the SOCC. This service provides for the facility, site connectivity, on-going support of server images for Disaster Recovery as a Service, and associated services. Metro Site Facilities are for the support of Virtual Server and Data Storage, providing Global/Metro Mirroring at a secondary near real time failover site within the Metro Columbus area.

2.3.3.9. Server Virtualization:

Server Virtualization is the practice of abstracting the physical hardware resources of compute, storage and networking of a host server and presenting those resources individually to multiple guest virtual servers contained in separate virtual environments. DAS OIT leverages the VMware vSphere platform to transform standardized hardware into this shared resource model that is capable providing solutions around availability, security and automation.
Server Virtualization includes:

- **DAS OIT Managed Basic Server Virtualization:** DAS OIT hosts the virtual server and manages the hardware/virtualization layer. DAS OIT is also responsible for managing the server's operating system (OS). This service includes 1 virtual CPU (vCPU), 1 GB of RAM and 50 GB of General Disk Storage used for the operating system.

Please explain how the State's Data Center Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

Deloitte's proposed solution is hosted on AWS cloud and managed by Deloitte. The cloud hosting infrastructure implements the required backup and data storage strategies.

2.3.4. Hosted Services

2.3.4.1. Database as a Service:

Database as a Service provides an enterprise database solution that is easy to use and simple to update without incurring the cost of setting up and maintaining an enterprise database environment through which scaling, load balancing, failover and backup can all be managed. DAS OIT Database Specialists ensure that all aspects of handling data are taken care of which includes, but is not limited to, storage, backups, tuning and security.

Current Database Solutions being offered:

- SQL Server
- Oracle
- DB2

Oracle Exadata DBaaS:

- **Starter/Small Database:** 2 Cores, 6GB Ram, 200GB min Storage, *Up to 2 databases
  Entry level database environment for small applications.
- **Medium Database:** 4 Cores, 8 GB Ram, 500GB Min Storage, *Up to 4 databases
  Medium sized database environment for DB consolidation.
- **Large Database:** 6 Cores, 12GB Ram, 1TB Min Storage, *Up to 6 Databases
  Optimal service for large, complex database and data warehouse environments.

*The maximum number of databases is dependent upon the database size and actual usage.

Based on the model the proposed service model for DAS OIT includes the following structure:

- **Small**: 2 Core = 1 billable unit per month.
- **Medium**: 4 Cores = 2 billable units per month.
- **Large**: 6 Cores = 3 billable units per month.

2.3.4.2. Database Support:

Database Support provides technical assistance for database implementation and usage. Services utilized may include any or all of the following service offerings: installation, upgrade and management of database software, database administration tools and packaged application database products, backup/recovery procedure implementation, monitoring, tuning and troubleshooting.

Please explain how the State's Hosted Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

Deloitte's proposed solution is a pre-configured solution hosted on AWS with its own Database.

2.3.5. IT Security Services

2.3.5.1. Secure Sockets Layer (SSL) Digital Certificate Provisioning:

SSL Digital Certificate Provisioning service provides SSL Certificate service across multiple enterprise service offerings. SSL certificates are used to provide communication security to various web sites and communications protocols over the internet (ex. Web Servers, Network Devices, Application Servers, Internet Information Server (IIS), Apache, F5 devices and Exchange servers). SSL Digital Certificate Provisioning supports the delegation of administration and reporting processes while leveraging a common portal.

In addition, please review the Security Supplement (Supplement S - State Information Security and Privacy Requirements and State Data Handling Requirements).

Please explain how the State's IT Security Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

Deloitte's proposed solution leverages third-party certificate service for implementing SSL communication within the solution.

2.3.6. IT Support Services

2.3.6.1. Enterprise End User Support:

Enterprise End User Support is a standardized, fully managed endpoint computing service. This Service uses enterprise tools and standards. This comprehensive service includes e-mail, network connectivity, device procurement, printer support, security policy maintenance, system monitoring, software updates and patching, software deployment to individuals and devices and inventory software and hardware. IT assets provided with the Enterprise End User Support include:

- Dedicated on-site technician
- Break/Fix
- Enterprise Image
- System Center Configuration Management (SCCM)
- Patch Management through SCCM
- Application packaging and deployment
- Asset management (hardware)
- Asset management (software)
- Application usage report provided upon request

2.3.6.2. Enterprise Virtual Desktop:

Enterprise Virtual Desktop service takes advantage of the Enterprise Private Cloud to store all electronic data via a virtual desktop. The service provides a platform with access to Microsoft Windows and State of Ohio business applications from any device, from any location, at any time.

The Enterprise Virtual Desktop service offers the following:

- **Hosted** - The unmanaged service provides an isolated and dedicated environment that is managed by DAS OIT. This hosted service includes a provisioning portal, a basic window image and a basic group policy for desktops but does not include management or deployment of specific software or desktop provisioning.
- **Managed** - The managed service provides an isolated and dedicated environment that is managed by DAS OIT including desktops and software deployment. The Managed service also includes all Hosted services, software packaging and updating, management of the operating system, deployments and updates.

Please explain how the State's IT Support Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

Deloitte will continue to utilize the State's IT Support Services for the proposed solution like they are being leveraged currently.

2.3.7. Messaging Services

2.3.7.1. Microsoft License Administration (Office 365):

The Office 365 service provides the ability to use email, Office 365 ProPlus, instant messaging, online meetings and web conferencing, and file storage all from the Cloud, allowing access to services virtually anytime and from anywhere and includes email archiving and eDiscovery services.

The Office 365 service provides licensing and support for email, Office 365 ProPlus (Outlook, Word, Excel, PowerPoint, Publisher, Skype for Business and OneNote), SharePoint, and OneDrive for Business. Microsoft Office Suite includes:

- Email in the Microsoft Cloud
- Office 365 ProPlus
- Skype for Business
- SharePoint Online
- OneDrive for Business

Please explain how the State's Messaging Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

Deloitte agrees to use the State's messaging services to maintain and manage project documentation, including the project schedule, technical specifications, test plans, and training documentation, and for instant messaging and online meetings. Using SharePoint as a repository will facilitate collaboration and information sharing among members of the project team.

2.3.8. Network Services

Offeror's solutions must work within the State's LAN / WAN infrastructure.

2.3.8.1. Ohio One Network:

The State of Ohio's One Network is a unified solution that brings together design, engineering, operations, service delivery, security, mobility, management, and network infrastructure to target and solve key government challenges by focusing on processes, procedures, consistency and accountability across all aspects of State, city and local government.

Ohio One Network can deliver an enterprise network access experience regardless of location or device and deliver a consistent, reliable network access method.

2.3.8.2. Secure Authentication:

The DAS OIT Secure Authentication service provides a managed two-factor User authentication solution. The authentication function requires the User to identify themselves with two unique factors, something they know and something they have, before they are granted access. Whether local or remote, this service ensures that only authorized individuals are permitted access to an environment.

2.3.8.3. Wireless as a Service:

Wireless as a Service is the IT Enterprise Wireless hosted network. This service is an all-inclusive enterprise level wireless LAN solution that offers guest, employee, voice and location-based services with 24/7 target availability.

Coverage is three tiered:

- Broad coverage – small number of Users with low throughput, i.e. public hot spot, warehouse.
- General data use – most common, general computing with robust data performance.
- High capacity use (Voice) – maximum capacity, high bandwidth Users, i.e. location and tracking service.

Please explain how the State's Network Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

Deloitte's proposed solution will be hosted on AWS and managed by Deloitte and will interface with State's system hosted on the State's Network.

2.3.9. Telephony Services

2.3.9.1. Voice Services – VoIP

The State of Ohio hosted cloud VoIP service, also known as NGTS (Next Generation Telephony Service) provides core telephony, voice mail, e911, collaboration, video, audio, conferencing and auto attendant functions. Optional services include automatic call distributor (ACD), interactive voice response (IVR), multi-channel contact center solutions and session initiation protocol (SIP) trunking among a variety of other features. The service was the first business class phone system to offer closed captioning for the hearing impaired, and also includes features for those with vision and mobility impairments. The following voice services are offered in addition to the State's hosted VoIP service:

2.3.9.2. Toll-Free Services:

A service provided to incur telephone charges for incoming calls to an 8xx number.

2.3.9.3. Automatic Caller Navigation and Contact Center Services (ACD/Contact) Centers:

Contact Center Enterprise allows callers to fill in CRM forms with information prior to an agent responding. With IVR and Advanced Data Collection, callers will spend less time in Call Queues. However, during high demand times, callers can be put on Virtual Hold allowing callers to receive a call back when agents become available. Call recording with screen capture allows the User to monitor, record, store, and QA calls, helping insure a consistent service experience.

Service also includes multi-channel communications including chat, text, SMS and email to afford those trying to contact the State the ability to contact the State in a variety of ways.

2.3.9.4. Call Recording Services:

Call Recording Services for new VoIP profiles or modifying existing profiles.

2.3.9.5. Conferencing

This service offers a conferencing service via telephone lines. It provides voice conferencing capabilities within the network and participants can also join in from outside the network.

2.3.9.6. Fax2Mail:

Fax2Mail is a “hosted” fax solution that allows organizations to seamlessly integrate inbound and outbound fax with their existing desktop email and back-office environments. Fax2Mail is completely “cloud-based” (SaaS), providing an easy to implement, easy to manage solution requiring no expenditures on hardware or software. Fax2Mail solves all faxing requirements, including inbound and out-bound fax, both at the computer desktop and from/to back-office systems, ERP applications, and electronic workflows.

2.3.9.7. Session Initiation Protocol (SIP) Call Paths:

Session Initiation Protocol Call Paths is used to allocate bandwidth. SIP Call paths:

- Provide existing telephony infrastructure with NGTS services.
- Extends infrastructure into the NGTS cloud.
- Leverages existing investment.
- Bridges the gap.
- All of the United States are Local Calls.
- Share video and collaboration.
- Leverage Toll Free offering.
- Centralized trunk savings.

2.3.9.8. Site Survivability:

Provides reliable communications via multi-feature redundancy for centralized call processing.

2.3.9.9. VoIP related Professional Services and Training:

Training services can be requested for VoIP telephone Users.
Professional services are also available for planning and migration of large contact centers, and for integration of contact centers with cloud services including Salesforce.

Please explain how the State's Voice/VoIP Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

We will leverage an efficient and transparent project change control process if the State desires Deloitte to implement communication services as listed in this section

Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements

If an offeror needs to request a variance from a State IT Policy, Standard or Service requirement outlined in this supplement, please provide a rationale and an overview for each request in the table below.

Section Reference	IT Policy, Standard or Service Requirement	Rationale for Proposed Variance from Requirement	Proposed Variance Overview
Example: **Section 3.3.2 Application Services - Enterprise eSignature Service**	**Example**: The offeror shall use the State's eSignature solution.	**Example:** An eSignature solution is already integrated into the proposed solution. Using the State's service would result in increased cost due to integration complexities, as well as additional testing and resource needs. It would also result in longer deliverable timeframe.	**Example:** The Offeror's eSignature solution provides the same capabilities as the State's required solution. The Offeror's solution includes a workflow component and an eSignature User interface.

Supplement S

State Information Security and Privacy Requirements

State Data Handling Requirements

Revision History:

Date:	Description of Change:	Version
10/01/2019	Updated the State Information Security and Privacy Requirements as well as the State Data Handling Requirements to align with current practices.	1.0

Table of Contents

Page

State Information Security, Privacy and Data Handling Requirements Instructions 1
Overview and Scope 1
State Requirements Applying to All Solutions 1
1. State Information Security and Privacy Standards and Requirements 2
1.1. The Offeror's Responsibilities 2
1.2 The State's Responsibilities 3
1.3. Periodic Security and Privacy Audits 3
1.3.1. State Penetration and Controls Testing 4
1.3.2. System Security Plan 7
1.3.3. Risk Assessment 10
1.4. Security and Data Protection 12
1.5. Protection of State Data 12
1.6. Handling the State's Data 13
1.7. Contractor Access to State Networks Systems and Data 16
1.8. State Network Access (VPN) 25
1.9. Portable Devices and Media 25
2. State and Federal Data Privacy Requirements 26
2.1 Contractor Requirements 26
2.2. Federal Tax Information (FTI) 27
2.2.1. IRS 1075 Performance Requirements 27
2.3.2. IRS 1075 Criminal/Civil Sanctions 29
2.4.3. Disclosure 30
2.5. Background Investigations of Contractor Personnel 31
3. Contractor Responsibilities Related to Reporting of Concerns, Issues and Security/Privacy Issues 33
3.1. General 33
3.2. Actual or Attempted Access or Disclosure 34
3.3. Unapproved Disclosures and Intrusions: Contractor Responsibilities 35
3.4. Security Incident Reporting and Indemnification Requirements 36
4. Security Review Services 38
4.1. Hardware and Software Assets 38
4.2. Security Standards by Device and Access Type 39
4.3. Boundary Defenses 39

4.4. Audit Log Reviews 40
4.5. Application Software Security 40
4.7. Account Access Privileges 43
4.8. Additional Controls and Responsibilities 43
Appendix A – Compensating Controls to Security and Privacy Supplement 45

Ohio | Department of Administrative Services
Office of Information Security and Privacy
Main Number: 614-644-9391
30 E Broad Street, 19th Floor
Columbus, Ohio 43215
infosec.ohio.gov

State Information Security, Privacy and Data Handling Requirements Instructions

When providing a response to this Supplement, please follow the instructions below and frame your response as it relates to your proposed solution e.g., cloud (Software as a Service, Platform as a Service, or Infrastructure as a Service), on-premises, or hybrid.

1. **After each specific requirement the offeror must provide a response on how the requirement will be met or indicate if it is not applicable and why.**

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement shall not be modified.

2. **In the event there is a security or privacy requirement outlined in this supplement that needs to be met by a compensating control, please identify it in Appendix A – Compensating Controls to Security and Privacy Requirements. Please be sure to provide a rationale for the change.**

Reference	Current Language	Contractor's Proposed Change	Rationale of Proposed Change
Example: **Supplement 2 - Page 11**	**Example**: Provide vulnerability management services for the Contractor's internal secure network connection, including supporting remediation for identified vulnerabilities as agreed. As a minimum, the Contractor must provide vulnerability scan results to the State **monthly**.	**Example:** Provide vulnerability management services for the Contractor's internal secure network connection, including supporting remediation for identified vulnerabilities as agreed. As a minimum, the Contractor must provide vulnerability scan results to the State **weekly**.	Per company policy vulnerability report are only provided to customers on a quarterly basis.

3. **Upon completion, please submit the security supplement responses with the proposal documentation.**

Overview and Scope

This supplement shall apply to the Contracts for all work, services, locations (e.g., cloud (Software as a Service, Platform as a Service, or Infrastructure as a Service), on-premises, or hybrid) along with the computing elements that the Contractor will perform, provide, occupy, or utilize in conjunction with the delivery of work to the State and any access to State resources in conjunction with the delivery of work.

The selected Contractor will accept the security and privacy requirements outlined in this supplement in their entirety as they apply to the services being provided to the State. The Contractor will be responsible for maintaining information security in environments under the Contractor's management and in accordance with State IT security policies and standards.

This scope shall specifically apply to:

- Major and minor projects, upgrades, updates, fixes, patches, and other software and systems inclusive of all State elements or elements under the Contractor's responsibility utilized by the State.
- Any systems development, integration, operations, and maintenance activities performed by the Contractor.
- Any authorized change orders, change requests, statements of work, extensions, or amendments to this contract.
- Contractor locations, equipment, and personnel that access State systems, networks or data directly or indirectly.
- Any Contractor personnel or sub-contracted personnel that have access to State confidential, personal, financial, infrastructure details or sensitive data.

The terms in this supplement are in addition to the Contract terms and conditions. In the event of a conflict for whatever reason, the highest standard contained in this contract shall prevail.

Please note that any proposed compensating controls to the security and privacy requirements outlined in this supplement are required to be identified in Appendix A – Compensating Controls to Security and Privacy Requirements. Contractors are asked not to make any changes to the language contained within this supplement.

State Requirements Applying to All Solutions

This section describes the responsibilities for both the selected Contractor and the State of Ohio as it pertains to State information security and privacy standards and requirements for all proposed solutions whether cloud, on-premises, or hybrid based. The Contractor will comply with State of Ohio IT security and privacy policies and standards as they apply to the services being provided to the State. A list of IT policy and standard links is provided in the State IT Policy and Standard Requirements and State IT Service Requirements supplement.

1. State Information Security and Privacy Standards and Requirements

The Contractor is responsible for maintaining the security of information in accordance with State security policies and standards. If the State is providing the network layer, the Contractor must be responsible for maintaining the security of the information in environment elements that are accessed, utilized, developed, or managed. In either scenario, the Contractor must implement information security policies, standards, and capabilities as set forth in statements of work and adhere to State policies and use procedures in a manner that does not diminish established State capabilities and standards.

1.1. The Offeror's Responsibilities

The offeror's responsibilities with respect to security services include the following, where applicable:

1.1.1. Support State IT security policies and standards, which includes the development, maintenance, updates, and implementation of security procedures with the State's review and approval, including physical access strategies and standards, User ID approval procedures, and a security incident action plan.

1.1.2. Support the implementation and compliance monitoring as per State IT security policies and standards.

1.1.3. If the Contractor identifies a potential issue with maintaining an "as provided" State infrastructure element in accordance with a more stringent State level security policy, the Contractor shall identify and communicate the nature of the issue to the State, and, if possible, outline potential remedies for consideration by the State.

1.1.4. Support intrusion detection and prevention, including prompt State notification of such events and reporting, monitoring, and assessing security events.

1.1.5. Provide vulnerability management services for the Contractor's internal secure network connection, including supporting remediation for identified vulnerabilities as agreed. At a minimum, the Contractor shall provide vulnerability scan results to the State monthly.

1.1.6. Develop, maintain, update, and implement security procedures, with State review and approval, including physical access strategies and standards, ID approval procedures and a security incident response plan.

1.1.7. Manage and administer access to the systems, networks, system software, systems files, State data, and end users if applicable.

1.1.8. Install and maintain current versions of system software security, assign and reset passwords per established procedures, provide the State access to create User IDs, suspend and delete inactive User IDs, research system security problems, maintain network access authority, assist in processing State security requests, perform security reviews to confirm that adequate security procedures are in place on an ongoing basis, provide incident investigation support (jointly with the State), and provide environment and server security support and technical advice.

1.1.9. Develop, implement, and maintain a set of automated and manual processes to ensure that data access rules are not compromised.

1.1.10. Perform physical security functions (e.g., identification badge controls and alarm responses) at the facilities under the Contractor's control.

1.2 The State's Responsibilities

The State will:

1.2.1. Develop, maintain, and update the State IT security policies, including applicable State information risk policies, standards, and procedures.

1.2.2. Provide the Contractor with contact information for security and program personnel for incident reporting purposes.

1.2.3. Provide a State resource to serve as a single point of contact, with responsibility for account security audits.

1.2.4. Support intrusion detection, prevention, and vulnerability scanning pursuant to State IT security policies.

1.2.5. Conduct a Security and Data Protection Audit, if deemed necessary, as part of the testing process.

1.2.6. Provide audit findings material for the services based upon the security policies, standards and practices in effect as of the effective date and any subsequent updates.

1.2.7. Assist the Contractor in performing a baseline inventory of User IDs for the systems for which the Contractor has security responsibility.

1.2.8. Authorize user IDs and passwords for State personnel for the system's software, software tools and network infrastructure systems and devices under Contractor management.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement shall not be modified.

[redacted]

1.3. Periodic Security and Privacy Audits

The State will be responsible for conducting periodic security and privacy audits and will generally utilize members of the Office of Information Security and Privacy, the Office of Budget and Management – Office of Internal Audit, and the Auditor of State, depending on the focus area of the audit. Should an audit issue or finding be discovered, the following resolution path shall apply:

If a security or privacy issue exists in any of the IT resources furnished to the Contractor by the State (e.g., code, systems, computer hardware and software), the State will have responsibility to address or resolve the issue. The State may elect to work with the Contractor, under mutually agreeable terms for resolution services or the State

may elect to address the issue independent of the Contractor. The Contractor is responsible for resolving any security or privacy issues that exist in any of the IT resources they provide to the State.

For in-scope environments and services, all new systems implemented or deployed by the Contractor must comply with State security and privacy policies and standards.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

[redacted]

1.3.1. State Penetration and Controls Testing

The State may, at any time in its sole discretion, elect to perform a Security and Data Protection Audit. This includes a thorough review of Contractor controls, security/privacy functions and procedures, data storage and encryption methods, backup/restoration processes, as well as security penetration testing and validation. The

State may utilize a third-party Contractor to perform such activities to demonstrate that all security, privacy, and encryption requirements are met.

State acceptance testing will not proceed until the Contractor cures, according to the State's written satisfaction, all findings, gaps, errors or omissions pertaining to the audit. Such testing will be scheduled with the Contractor at a mutually agreed upon time.

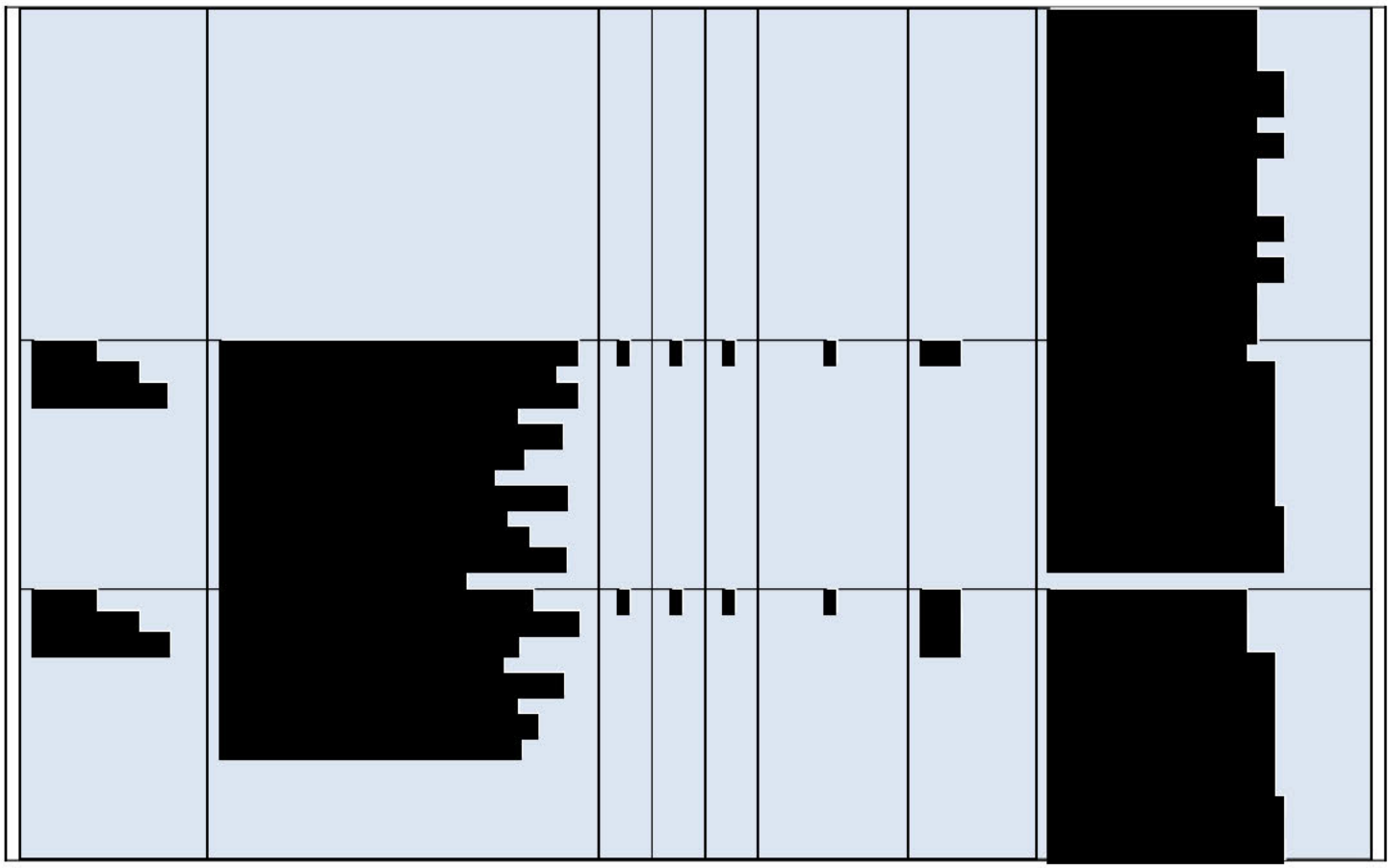
Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.3.2. System Security Plan

A completed System Security Plan must be provided by the Contractor to the State and the primary point of contact from the Office of Information Security and Privacy no later than the end of the project development phase of the System Development Life Cycle (SDLC). The plan must be updated annually or when major changes occur within the solution. The templates referenced below are the required format for submitting security plans to the State.

Ohio Security Plan Template.docx

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.



1.3.3. Risk Assessment

A Risk Assessment report completed within the past 12 months must be provided to the State and the primary point of contact from the Office of Information Security and Privacy no later than the project development phase of the System Development Life Cycle (SDLC). A new risk assessment must be conducted every two years, or as a result of significant changes to infrastructure, a system or application environment, or following a significant security incident.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.4. Security and Data Protection

All solutions must classify data per State of Ohio IT-13 Data Classification policy and per the sensitivity and criticality, must operate at the appropriate baseline (low, moderate, high) as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations" (current, published version), be consistent with Federal Information Security Management Act ("FISMA 2014") requirements, and offer a customizable and extendable capability based on open-standards APIs that enable integration with third party applications. The solution must provide the State's systems administrators with 24x7 visibility into the services through a real-time web-based "dashboard" capability that enables them to monitor, in real or near real time, the services' performance against the established service level agreements and promised operational parameters.

If the solution is cloud based, the Contractor must obtain an annual audit that meets the American Institute of Certified Public Accountants (AICPA) Statements on Standards for Attestation Engagements ("SSAE") No. 16, Service Organization Control 1 Type 2 and Service Organization Control 2 Type 2. The audit must cover all operations pertaining to the Services covered by this Agreement. The audit will be at the sole expense of the Contractor and the results must be provided to the State within 30 days of its completion each year.

At no cost to the State, the Contractor must immediately remedy any issues, material weaknesses, or other items identified in each audit as they pertain to the Services.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

[redacted]

1.5. Data

1.5.1. "State Data" includes all data and information created by, created for, or related to the activities of the State and any information from, to, or related to all persons that conduct business or personal activities with the State, including, but not limited to Sensitive Data.

1.5.2. "Sensitive Data" is any type of data that presents a high or moderate degree of risk if released or disclosed without authorization. Sensitive Data includes but not limited to:

1.5.2.1. Certain types of personally identifiable information (PII) that is also sensitive, such as medical information, social security numbers, and financial account numbers.

1.5.2.2. Federal Tax Information (FTI) under IRS Special Publication 1075,

1.5.2.3. Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA)

1.5.2.4. Criminal Justice Information (CJI) under Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy.

1.5.2.5. The data may also be other types of information not associated with an individual such as security and infrastructure records, trade secrets, and business bank account information.

1.6. Protection and Handling the State's Data

To protect State Data as described in this contract, the Contractor must use due diligence to ensure computer and telecommunications systems and services involved in storing, using, or transmitting State Data are secure and to protect State Data from unauthorized disclosure, modification, use or destruction.

To accomplish this, the Contractor must adhere to the following requirements regarding State Data:

1.6.1. Maintain in confidence State Data it may obtain, maintain, process, or otherwise receive from or through the State in the course of the contract.

1.6.2. Use and permit its employees, officers, agents, and subcontractors to use any State Data received from the State solely for those purposes expressly contemplated by the contract.

1.6.3. Not sell, rent, lease, disclose, or permit its employees, officers, agents, and sub-contractors to sell, rent, lease, or disclose, any such State Data to any third party, except as permitted under this contract or required by applicable law, regulation, or court order.

1.6.4. Take all commercially reasonable steps to (a) protect the confidentiality of State Data received from the State and (b) establish and maintain physical, technical, and administrative safeguards to prevent unauthorized access by third parties to State Data received by the Contractor from the State.

1.6.5. Apply appropriate risk management techniques to balance the need for security measures against the sensitivity of the State Data.

1.6.6. Ensure that its internal security policies, plans, and procedures address the basic security elements of confidentiality, integrity, and availability of State Data.

1.6.7. Align with existing State Data security policies, standards and procedures designed to ensure the following:

1.6.7.1. Security and confidentiality of State Data

1.6.7.2. Protection against anticipated threats or hazards to the security or integrity of State Data

1.6.7.3. Protection against the unauthorized access to, disclosure of, or use of State Data

1.6.8. Suggest and develop modifications to existing data security policies and procedures or draft new data security policies and procedures when gaps are identified.

1.6.9. Maintain appropriate access control and authorization policies, plans, and procedures to protect system assets and other information resources associated with State Data.

1.6.10. Give access to State Data only to those individual employees, officers, agents, and sub-contractors who reasonably require access to such information in connection with the performance of Contractor's obligations under this contract.

1.6.11. Maintain appropriate identification and authentication processes for information systems and services associated with State Data.

1.6.12. Any Sensitive Data at rest, transmitted over a network, or taken off-site via portable/removable media must be encrypted pursuant to the State's data encryption standard, Ohio IT Standard ITS-SEC-01, "Data Encryption and Cryptography," and Ohio Administrative Policy IT-14, "Data Encryption and Securing State Data."

1.6.13. Any data encryption requirement identified in this supplement means encryption that complies with National Institute of Standards and Technology's Federal Information Processing Standard 140-2 as demonstrated by a valid FIPS certificate number.

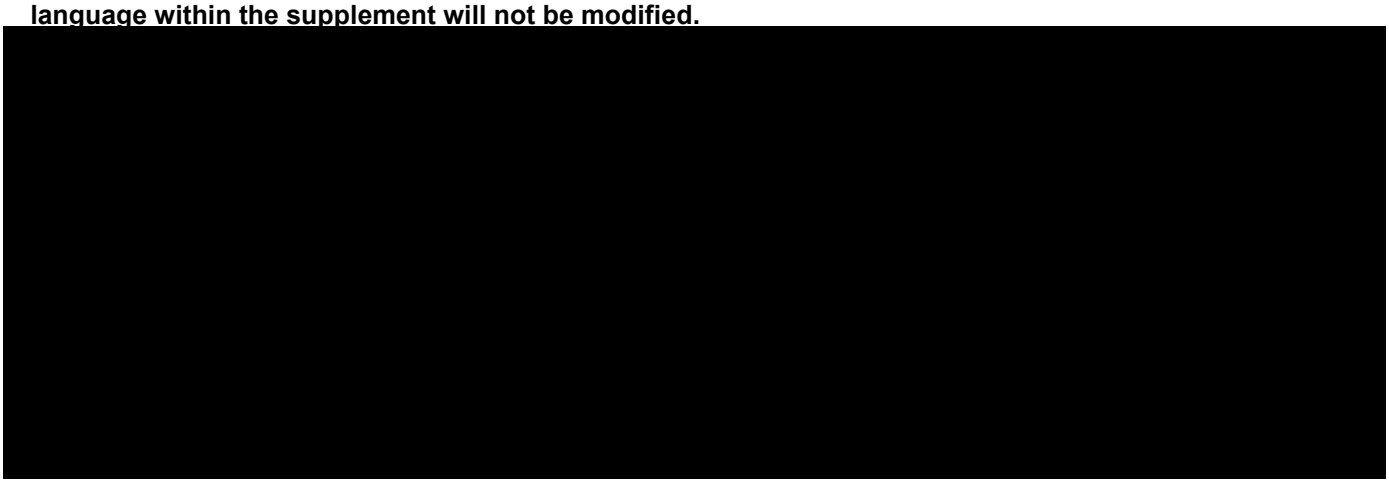
1.6.14. Maintain plans and policies that include methods to protect against security and integrity threats and vulnerabilities, as well as detect and respond to those threats and vulnerabilities.

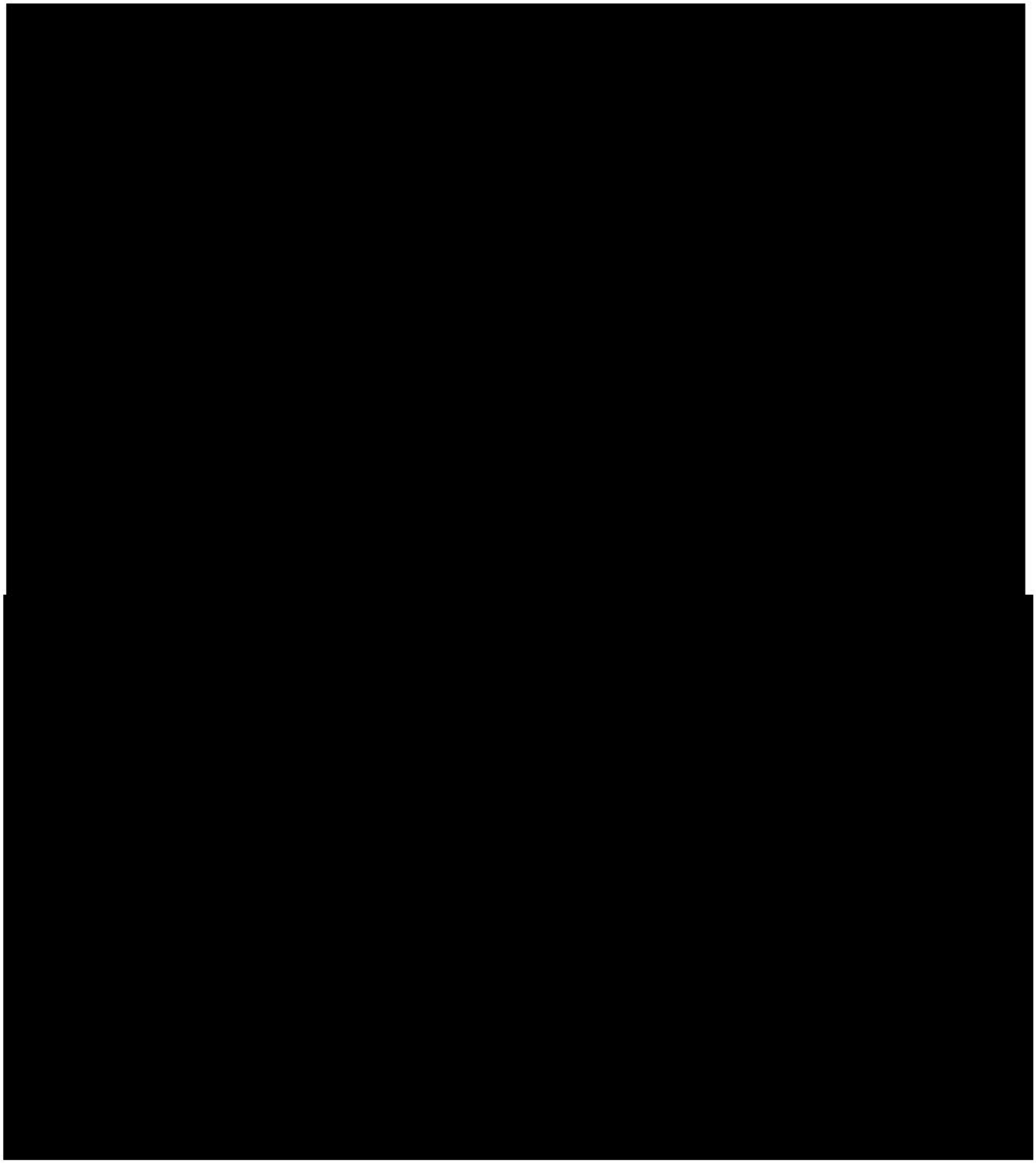
1.6.15. Implement and manage security audit logging on information systems, including computers and network devices.

1.6.16. Cooperate with any attempt by the State to monitor Contractor's compliance with the foregoing obligations as reasonably requested by the State. The State will be responsible for all costs incurred by the Contractor for compliance with this provision of this subsection.

1.6.17 Upon request by the State, promptly destroy or return to the State, in a format designated by the State, all State Data received from or through the State.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.





1.7. Contractor Access to State Network Systems and Data

The Contractor must maintain a robust boundary security capability that incorporates generally recognized system hardening techniques. This includes determining which ports and services are required to support access to systems that hold State Data, limiting access to only these ports, and disabling all others.

To do this, the Contractor must:

1.7.1 Use assets and techniques such as properly configured firewalls, a demilitarized zone for handling public traffic, host-to-host management, Internet protocol specification for source and destination, strong authentication, encryption, packet filtering, activity logging, and implementation of system security fixes and patches as they become available.

1.7.2. Use multifactor authentication to limit access to systems that contain Sensitive Data, such as Personally Identifiable Information.

1.7.3. Assume all State Data is both confidential and critical for State operations. The Contractor's security policies, plans, and procedures for the handling, storage, backup, access, and, if appropriate, destruction of State Data must be commensurate to this level of sensitivity unless the State instructs the Contractor otherwise in writing.

1.7.4. Employ appropriate intrusion and attack prevention and detection capabilities. Those capabilities must track unauthorized access and attempts to access State Data, as well as attacks on the Contractor's infrastructure associated with the State Data. Further, the Contractor must monitor and appropriately address information from its system tools used to prevent and detect unauthorized access to and attacks on the infrastructure associated with the State Data.

1.7.5. Use appropriate measures to ensure that State Data is secure before transferring control of any systems or media on which State data is stored. The method of securing the State Data must be in alignment with the required data classification and risk assessment outcomes, and may include secure overwriting, destruction, or encryption of the State data before transfer of control in alignment with NIST SP 800-88. The transfer of any such system or media must be reasonably necessary for the performance of the Contractor's obligations under this contract.

1.7.6. Have a business continuity plan in place that the Contractor tests and updates no less than annually. The plan must address procedures for responses to emergencies and other business interruptions. Part of the plan must address backing up and storing data at a location sufficiently remote from the facilities at which the Contractor maintains State Data in case of loss of State Data at the primary site. The Contractor's backup solution must include plans to recover from an intentional deletion attempt by a remote attacker exploiting compromised administrator credentials.

The plan also must address the rapid restoration, relocation, or replacement of resources associated with the State Data in the case of a disaster or other business interruption. The Contractor's business continuity plan must address short- and long-term restoration, relocation, or replacement of resources that will ensure the smooth continuation of operations related to the Sensitive Data. Such resources may include, among others, communications, supplies, transportation, space, power and environmental controls, documentation, people, data, software, and hardware. The Contractor also must provide for reviewing, testing, and adjusting the plan on an annual basis.

1.7.7. Not allow State Data to be loaded onto portable computing devices or portable storage components or media unless necessary to perform its obligations under this contract. If necessary, for such performance, the Contractor may permit State Data to be loaded onto portable computing devices or portable storage components or media only if adequate security measures are in place to ensure the integrity and security of State Data. Those measures must include a policy on physical security and appropriate encryption for such devices to minimize the risk of theft and unauthorized access as well as a prohibition against viewing sensitive or confidential data in public or common areas.

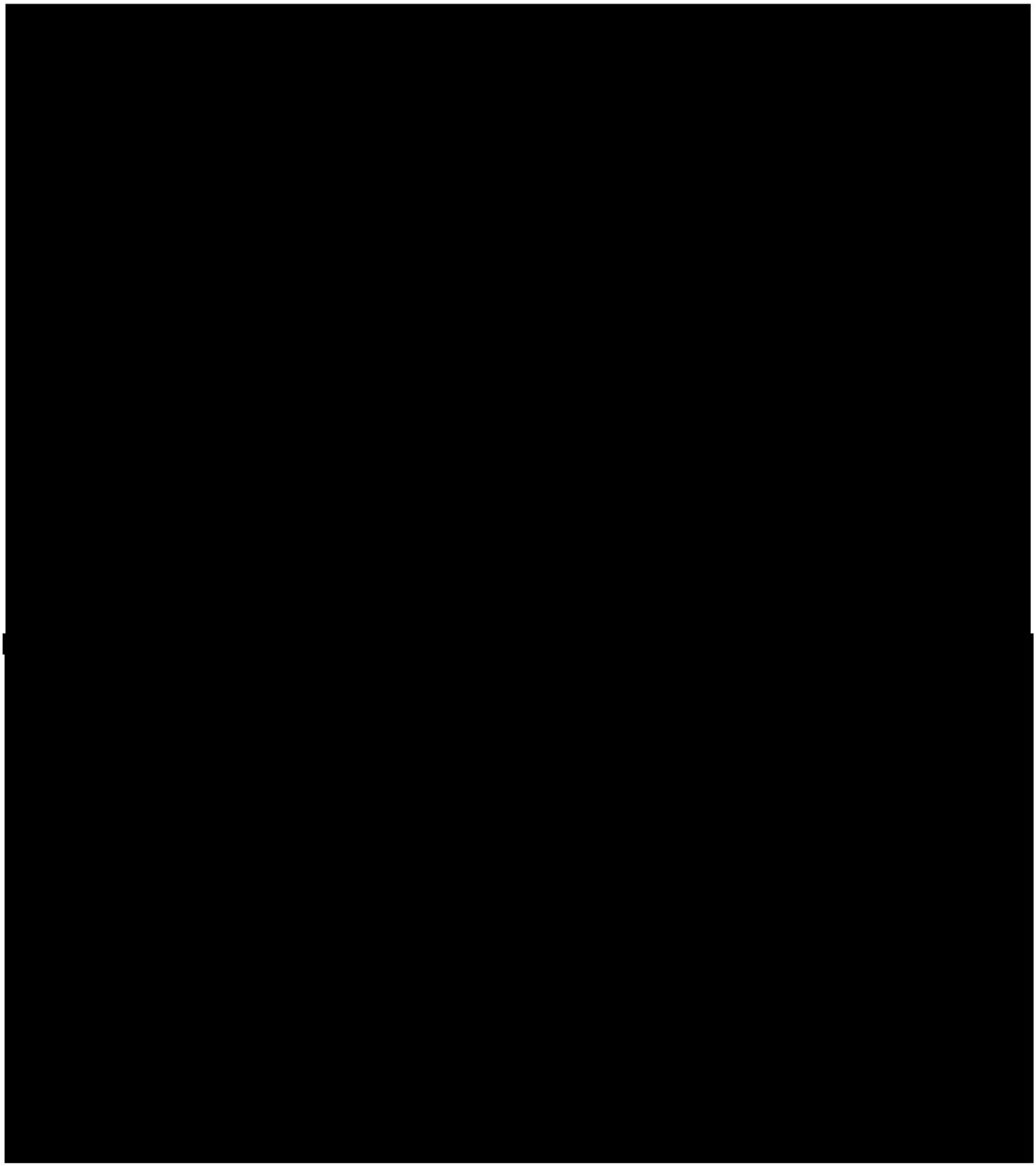
1.7.8. Ensure that portable computing devices have anti-virus software, personal firewalls, and system password protection. In addition, State Data must be encrypted when stored on any portable computing or storage device or media or when transmitted across any data network.

1.7.9. Maintain an accurate inventory of all such devices and the individuals to whom they are assigned.

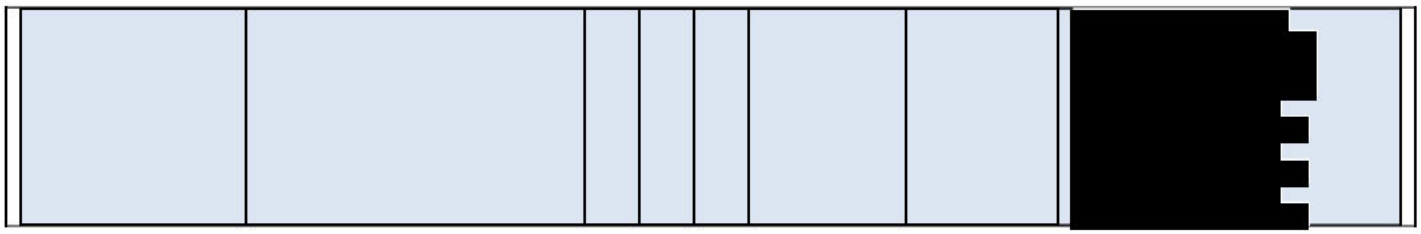
Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

[redacted]

[redacted]



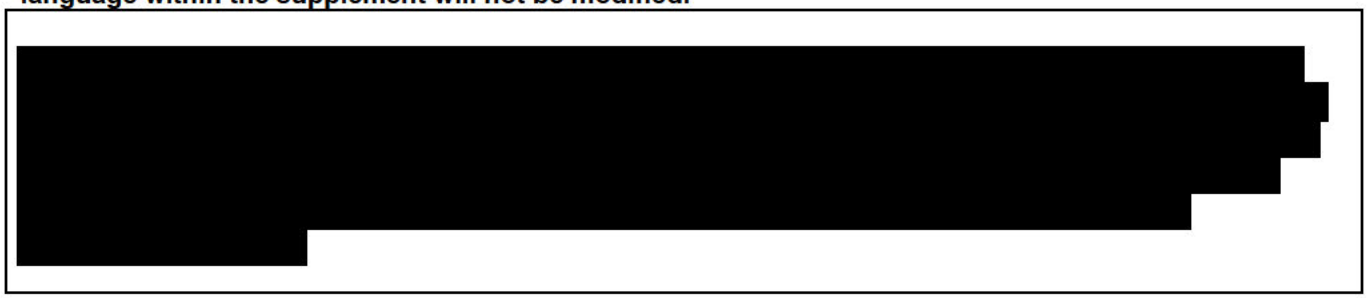
[redacted]



1.8. State Network Access (VPN)

Any remote access to State systems and networks, Contractor or otherwise, must employ secure data transmission protocols, including transport layer security (TLS) and public key authentication, signing and/or encryption. In addition, any remote access solution must use Secure Multipurpose Internet Mail Extensions (S/MIME) to provide encryption and non-repudiation services through digital certificates and the provided public key infrastructure (PKI). Multifactor authentication must be employed for users with privileged network access by State provided solutions.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.



1.9. Portable Devices and Media

The Contractor must have reporting requirements for lost or stolen portable computing devices authorized for use with State Data and must report any loss or theft of such devices to the State in writing as defined in Section 3 Contractor Responsibilities Related to Reporting of Concerns, Issues and Security/Privacy Issues. The Contractor must have a written policy that defines procedures for how the Contractor must detect, evaluate, and respond to adverse events that may indicate an incident or an attempt to attack or access State Data or the infrastructure associated with State Data.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

2. State and Federal Data Privacy Requirements

All systems and services must be designed and must function according to Fair Information Practice Principles (FIPPS), which are transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, accountability, and auditing.

To the extent that personally identifiable information (PII) in a system is "protected health information" under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, the FIPPS principles must be implemented in alignment with the HIPAA Privacy Rule. To the extent that there is PII in a system that is not "protected health information" under HIPAA, the FIPPS principles must still be implemented and, when applicable, aligned to other laws or regulations.

2.1 Contractor Requirements

The Contractor specifically agrees to comply with state and federal confidentiality and information disclosure laws, rules and regulations applicable to the work associated with this Contract including but not limited to:

2.1.1. United States Code 42 USC 1320d through 1320d-8 (HIPAA).

2.1.2. Code of Federal Regulations for Public Health and Public Welfare: 42 CFR 431.300, 431.302, 431.305, 431.306, 435.945, 45 CFR164.502 (e) and 164.504 (e).

2.1.3. Ohio Revised Code (ORC) 1347.01, 1347.04 through 1347.99, 2305.24, 2305.251, 3701.243, 3701.028, 4123.27, 5101.26, 5101.27, 5160.39, 5168.13, and 5165.88.

2.1.4. Corresponding Ohio Administrative Code Rules and Updates.

2.1.5. Systems and services must support and comply with the State's security operational support model, which is aligned to NIST SP 800-53 (current, published version).

2.1.6. IRS Publication 1075, Tax Information Security Guidelines for federal, state, and local agencies.

2.1.7. Criminal Justice Information Systems Policy.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

[redacted]

2.2. Federal Tax Information (FTI)

All computer systems receiving, processing, storing, or transmitting Federal Tax Information (FTI) must meet the requirements defined in IRS Publication 1075.

2.2.1. IRS 1075 Performance Requirements:

In the performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

2.2.1.1. All work involving FTI will be done under the supervision of the Contractor or the Contractor's employees.

2.2.1.2. The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.

2.2.1.3. Any federal tax return or return information made available in any format shall be used only for the purposes of performing this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the Contractor is prohibited.

2.2.1.4. All federal tax returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

2.2.1.5. The Contractor certifies that the IRS data processed during the performance of this contract will be completely purged from all data storage components of its computer facility, and no output will be retained by the Contractor after the work is completed. If immediate purging of all data storage components is not possible, the Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosure.

2.2.1.6. Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the State or its designee. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the State or its designee with a Statement containing the date of destruction, description of material destroyed, and the method used.

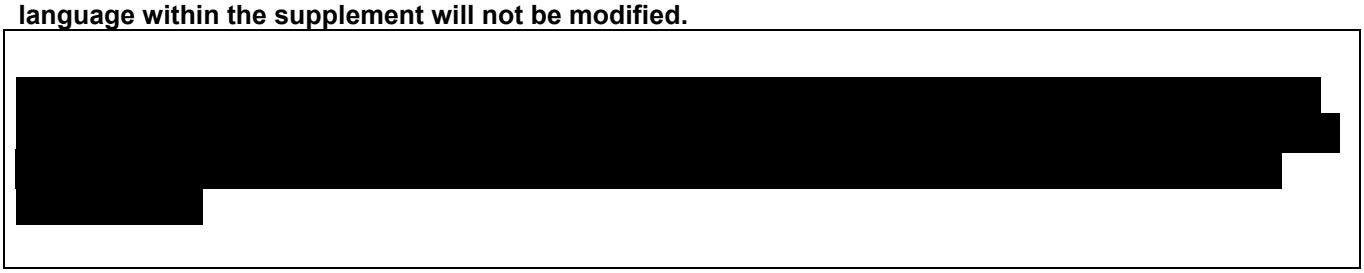
2.2.1.7. All computer systems receiving, processing, storing or transmitting FTI must meet the requirements defined in the IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operations, and technical IRS 1075 controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.

2.2.1.8 No work involving Federal Tax Information furnished under this contract will be subcontracted without prior written approval of the IRS.

2.2.1.9. The Contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

The agency will have the right to void the Contract if Contractor fails to provide the safeguards described above.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.



2.2.2. IRS 1075 Criminal/Civil Sanctions

2.2.2.1. Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

2.2.2.2. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of the officer or employee (United States for Federal employees) in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431.

2.2.2.3. Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to Contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a Contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

2.2.3. Inspection

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the Contractor for inspection of the facilities and operations performing any work under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual, and/or automated scanning tools to perform compliance and vulnerability assessment of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the Contractor is found to be noncompliant with contract safeguards.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

[redacted]

2.3. Disclosure

Disclosure to Third Parties. This Contract must not be deemed to prohibit disclosures in the following cases:

2.3.1. Required by applicable law, regulation, court order or subpoena; provided that, if the Contractor or any of its representatives are ordered or requested to disclose any information provided by the State, whether Sensitive Data or otherwise, pursuant to court or administrative order, subpoena, summons, or other legal process or otherwise believes that disclosure is required by any law, ordinance, rule or regulation, Contractor must notify the State within 24 hours in order that the State may have the opportunity to seek a protective order or take other appropriate action. Contractor must also cooperate in the State's efforts to obtain a protective order or other reasonable assurance that confidential treatment will be accorded the information provided by the State. If, in the absence of a protective order, Contractor is compelled as a matter of law to disclose the information provided by the State, Contractor may disclose to the party compelling disclosure only the part of such information as is required by law to be disclosed (in which case, prior to such disclosure, Contractor must advise and consult with the State and its counsel as to the scope of such disclosure and the nature of wording of such disclosure) and Contractor must use commercially reasonable efforts to obtain confidential treatment for the information:

2.3.1.1. To State auditors or regulators.

2.3.1.2. To service providers and agents of either party as permitted by law, provided that such service providers and agents are subject to binding confidentiality obligations.

2.3.1.3. To the professional advisors of either party, provided that such advisors are obligated to maintain the confidentiality of the information they receive.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

2.4. Background Investigations of Contractor Personnel

Contractor agrees that (1) the State of Ohio will conduct background investigations on Contractor personnel who will perform Sensitive Services (as defined below), and (2) no ineligible personnel will perform Sensitive Services under this contract. The term "ineligible personnel" means any person who (a) has been convicted at any time of any criminal offense involving dishonesty, a breach of trust, money laundering, or who has entered into a pre-trial diversion or similar program in connection with a prosecution for such offense, (b) is named by the Office of Foreign Asset Control (OFAC) as a Specially Designated National, or (c) has been convicted of a felony.

"Sensitive Services" means those services that (i) require access to customer, consumer, or State employee information, (ii) relate to the State's computer networks, information systems, databases or secure facilities under circumstances that would permit modifications to such systems, or (iii) involve unsupervised access to secure facilities.

Contractors who will have access to Federal Tax Information (FTI) or Criminal Justice Information (CJI) must complete a background investigation that is favorably adjudicated, prior to being permitted to access the information. In addition, existing Contractors with access to FTI or CJI that have not completed a background investigation within the last 5 years must complete a background investigation that is favorably adjudicated, prior to being permitted to access the information.

FTI or criminal justice background investigations will include:

2.4.1. FBI Fingerprinting (FD-258)

2.4.2. Local law enforcement agencies where the employee has lived, worked and/or attended school within the last five years

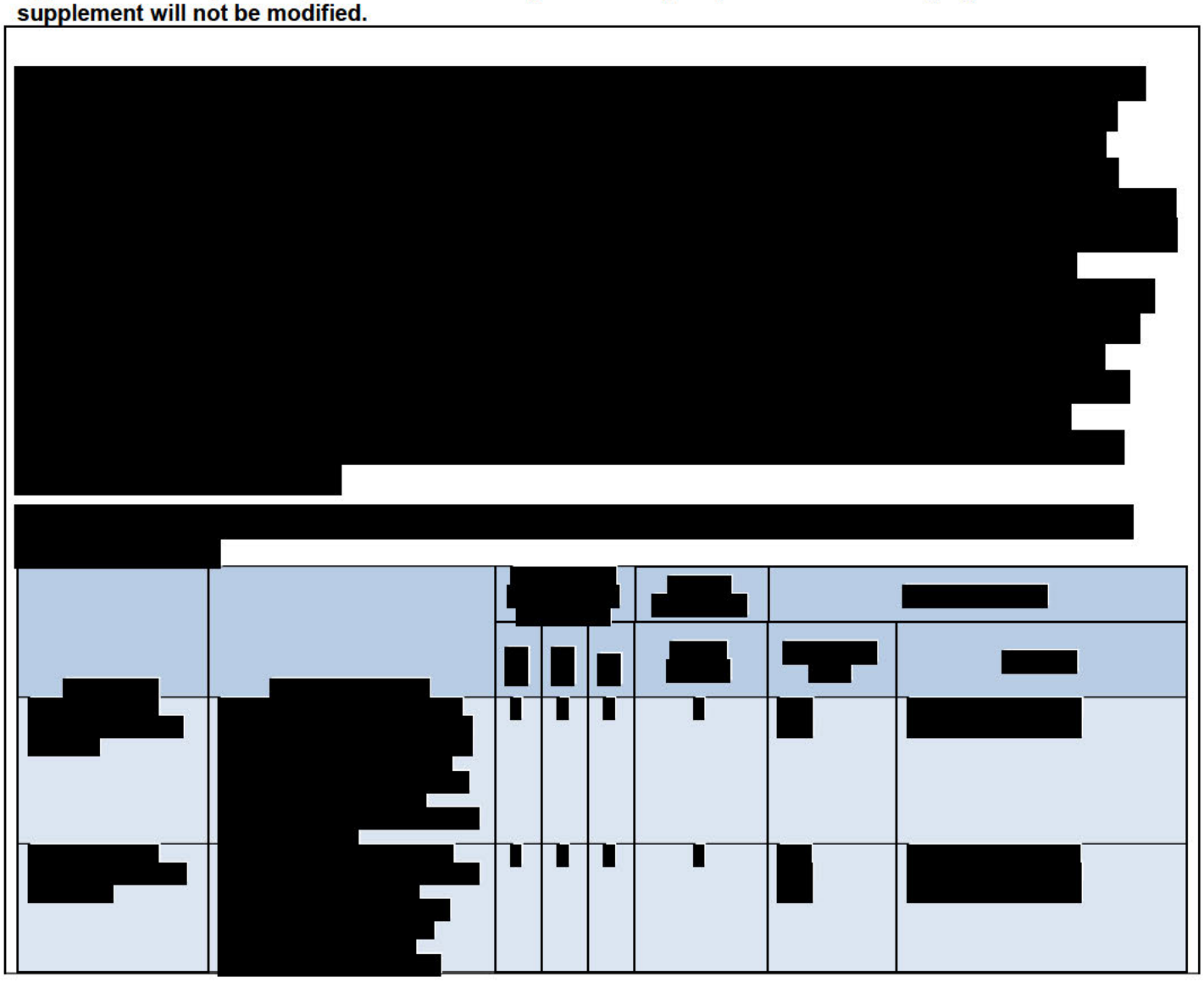
2.4.3. Citizenship/residency eligibility to legally work in the United States

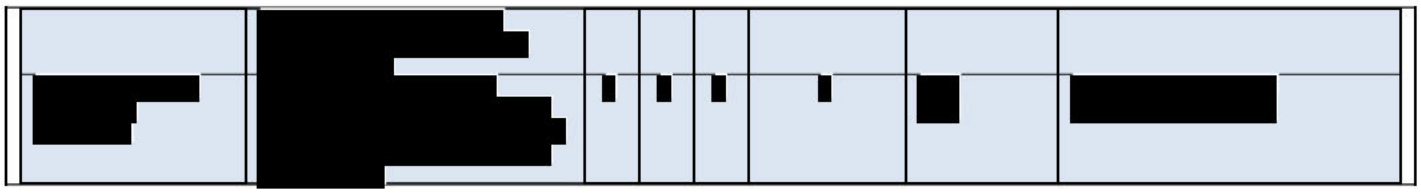
2.4.4. New employees must complete USCIS Form I-9, which must be processed through the Federal E-Verify system

2.4.5. FTI training, with a 45 day wait period

In the event that the Contractor does not comply with the terms of this section, the State may, in its sole and absolute discretion, terminate this Contract immediately without further liability.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.





3. Contractor Responsibilities Related to Reporting of Concerns, Issues, and Security/Privacy Issues

3.1. General

If, over the course of the Contract a security or privacy issue arises, whether detected by the State, a State auditor, or the Contractor, that was not existing within an in-scope environment or service prior to the commencement of any contracted service associated with this Contract, the Contractor must:

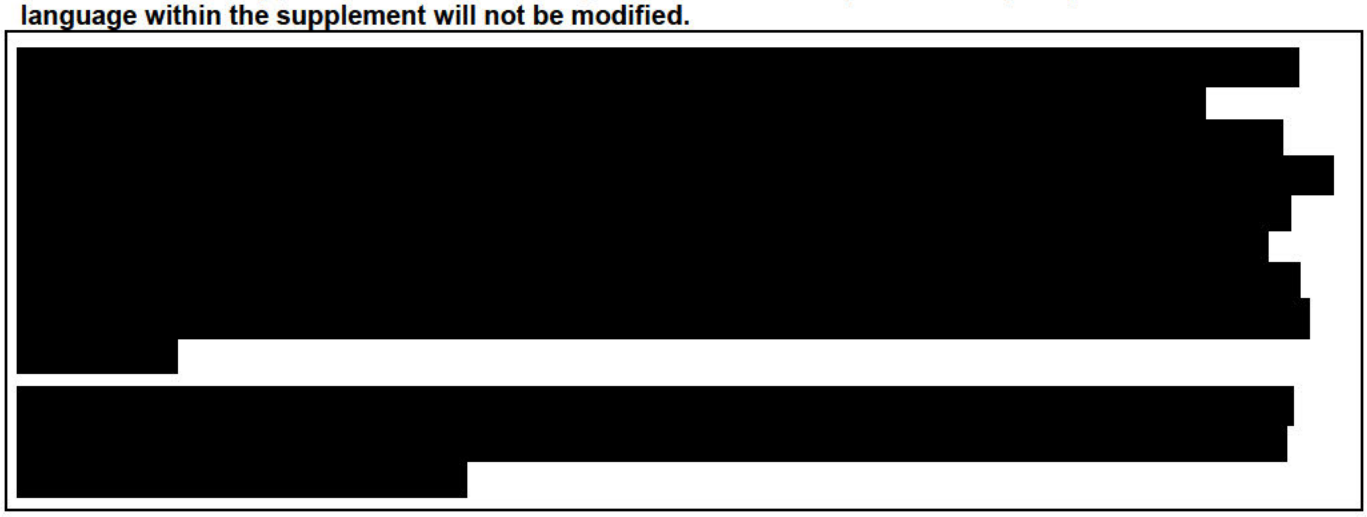
3.1.1. Notify the State of the issue or acknowledge receipt of the issue within two (2) hours.

3.1.2. Within forty-eight (48) hours from the initial detection or communication of the issue from the State, present a potential exposure or issue assessment document to the State account representative and the State Chief Information Security Officer with a high-level assessment as to resolution actions and a plan.

3.1.3. Within four (4) calendar days, and upon direction from the State, implement, to the extent commercially reasonable, measures to minimize the State's exposure to the security or privacy issue until such time as the issue is resolved.

3.1.4. Upon approval from the State, implement a permanent repair to the identified issue at the Contractor's cost.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.



[redacted]

3.2. Actual or Attempted Access or Disclosure

If the Contractor determines that there is any actual, attempted or suspected theft of, accidental disclosure of, loss of, or inability to account for any Sensitive Data by the Contractor or any of its Subcontractors (collectively "Disclosure") and/or any unauthorized intrusions into Contractor's or any of its Subcontractor's facilities or secure systems (collectively "Intrusion"), Contractor must immediately:

3.2.1. Notify the State within two (2) hours of the Contractor becoming aware of the unauthorized disclosure or intrusion.

3.2.2. Investigate and determine if an intrusion and/or disclosure has occurred.

3.2.3. Fully cooperate with the State in estimating the effect of the disclosure or intrusion and fully cooperate to mitigate the consequences of the disclosure or intrusion.

3.2.4. Specify corrective action to be taken.

3.2.5. Take corrective action to prevent further disclosure and/or intrusion.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

[redacted]

3.3. Unapproved Disclosures and Intrusions: Contractor Responsibilities

The following are the responsibility of the Contractor to provide at its own cost:

3.3.1. The Contractor must, as soon as is practical, make a report to the State including details of the disclosure and/or intrusion and the corrective action the Contractor has taken to prevent further disclosure and/or intrusion. The Contractor must, in the case of a disclosure, cooperate fully with the State to notify the affected persons as to the facts and circumstances of the disclosure of the Sensitive Data. Additionally, the Contractor must cooperate fully with all government regulatory agencies and/or law enforcement agencies that have jurisdiction to investigate a disclosure and/or any known or suspected criminal activity.

3.3.2. If, over the course of delivering services to the State under this statement of work for in-scope environments, the Contractor becomes aware of an issue, or a potential issue that was not detected by security and privacy teams, the Contractor must notify the State within two (2) hours. This notification must not minimize the more stringent service level contracts pertaining to security scans and breaches contained herein, which due to the nature of an active breach must take precedence over this notification. The State may elect to work with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.

3.3.3. If the Contractor identifies a potential issue with maintaining an “as provided” State infrastructure element in accordance with a more stringent State level security policy, the Contractor must identify and communicate the nature of the issue to the State, and, if possible, outline potential remedies.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

[redacted]

3.4. Security Incident Reporting and Indemnification Requirements

3.4.1. The Contractor must report any security incident of which it becomes aware. For the purposes of this document, "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. It does not mean unsuccessful log-on attempts, denial of service attacks, unsuccessful network attacks such as pings, probes of firewalls, port scans, or any combination of those, as long as there is no unauthorized access, acquisition, use, or disclosure of Sensitive Data as a result.

3.4.2. In the case of an actual security incident that may have compromised Sensitive Data, the Contractor must notify the State in writing within two (2) hours of the Contractor becoming aware of the breach. The Contractor is required to provide the best available information from the investigation.

3.4.3. In the case of a suspected incident, the Contractor must notify the State in writing within twenty-four (24) hours of the Contractor becoming aware of the suspected incident. The Contractor is required to provide the best available information from the investigation.

3.4.4. The Contractor must fully cooperate with the State to mitigate the consequences of an incident/suspected incident at the Contractor's own Cost. This includes any use or disclosure of the Sensitive Data that is inconsistent with the terms of this Contract and of which the Contractor becomes aware, including but not limited to, any discovery of a use or disclosure that is not consistent with this contract by an employee, agent, or Subcontractor of the Contractor.

3.4.5. The Contractor must give the State full access to the details of the breach/suspected breach and assist the State in making any notifications to potentially affected people and organizations that the State deems are necessary or appropriate at the Contractor's own cost.

3.4.6. The Contractor must document and provide incident reports for all such incidents/suspected incidents to the State. The Contractor must provide updates to incident reports until the investigation is complete at the Contractor's own cost. At a minimum, the incident/suspected incident reports will include:

3.4.6.1. Data elements involved, the extent of the Data involved in the incident, and the identification of affected individuals, if applicable.

3.4.6.2. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed State Data, or to have been responsible for the incident.

3.4.6.3. A description of where the State Data is believed to have been improperly transmitted, sent, or utilized, if applicable.

3.4.6.4. A description of the probable causes of the incident.

3.4.6.5. A description of the proposed plan for preventing similar future incidents, including ongoing risk remediation plan approval.

3.4.6.6. Whether the Contractor believes any federal or state laws requiring notifications to individuals are triggered.

3.4.7. In addition to any other liability under this contract related to the Contractor's improper disclosure of State Data, and regardless of any limitation on liability of any kind in this Contract, the Contractor will be responsible for acquiring one year's identity theft protection service on behalf of any individual or entity whose Sensitive Data is compromised while it is in the Contractor's possession. This service will be provided at Contractor's own cost. Such identity theft protection must provide coverage from all three major credit reporting agencies and provide immediate notice through phone or email of attempts to access the individual's credit history through those services.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

[redacted]

[redacted]

4. Security Review Services

As part of a regular Security Review process, the Contractor will include the following reporting and services to the State:

4.1. Hardware and Software Assets

The Contractor will support the State in defining and producing specific reports for both hardware and software assets. At a minimum this includes:

4.1.1. Deviations from the hardware baseline.

4.1.2. Inventory of information types by hardware device.

4.1.3. Software inventory compared against licenses (State purchased).

4.1.4. Software versions and then scans of versions against patches distributed and applied.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

[redacted]

4.2. Security Standards by Device and Access Type

The Contractor must:

4.2.1. Document security standards by device type and execute regular scans against these standards to produce exception reports.

4.2.2. Document and implement a process for any required remediation.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

[redacted]

4.3. Boundary Defenses

The Contractor must:

4.3.1. Work with the State to support the denial of communications to/from known malicious IP addresses.

4.3.2. Ensure that the system network architecture separates internal systems from DMZ and extranet systems.

4.3.3. Require the use of two-factor authentication for remote login.

4.3.4. Support the State's monitoring and management of devices remotely logging into the internal network.

4.3.5. Support the State in the configuration of firewall session tracking mechanisms for addresses that access the solution.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

[redacted]

4.4. Audit Log Reviews

The Contractor must:

4.4.1. Work with the State to review and validate audit log settings for hardware and software.

4.4.2. Ensure that all systems and environments have adequate space to store logs.

4.4.3. Work with the State to devise and implement profiles of common events from given systems to reduce false positives and rapidly identify active access.

4.4.4. Provide requirements to the State to configure operating systems to log access control events.

4.4.5. Design and execute bi-weekly reports to identify anomalies in system logs.

4.4.6. Ensure logs are written to write-only devices for all servers or a dedicated server managed by another group.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

[redacted]

4.5. Application Software Security

The Contractor must:

4.5.1. Perform configuration review of operating system, application, and database settings.

4.5.2. Ensure software development personnel receive training in writing secure code.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A – Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

[redacted]

[redacted]

4.6. System Administrator Access

The Contractor must:

4.6.1. Inventory all administrative passwords (application, database, and operating system level).

4.6.2. Implement policies to change default passwords in accordance with State policies, following any transfer or termination of personnel (State, existing Materials and Supplies Vendor, or Contractor).

4.6.3. Configure administrative accounts to require regular password changes.

4.6.4. Ensure user and service level accounts have cryptographically strong passwords.

4.6.5. Store passwords in a hashed or encrypted format.

4.6.6. Ensure administrative accounts are used only for administrative activities.

4.6.7. Implement focused auditing of administrative privileged functions.

4.6.8. Configure systems to log entry and alert when administrative accounts are modified.

4.6.9. Segregate administrator accounts based on defined roles.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

[redacted]

4.7. Account Access Privileges

The Contractor must, in alignment with policy requirements:

4.7.1. Review and disable accounts not associated with a business process.

4.7.2. Create a daily report that includes locked out accounts, disabled accounts, etc.

4.7.3. Implement a process for revoking system access.

4.7.4. Automatically log off users after a standard period of inactivity.

4.7.5. Monitor account usage to determine dormant accounts.

4.7.6. Monitor access attempts to deactivated accounts through audit logging.

4.7.7. Profile typical account usage and implement or maintain profiles to ensure that security profiles are implemented correctly and consistently.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

[redacted]

4.8. Additional Controls and Responsibilities

The Contractor must meet with the State no less frequently than annually to:

4.8.1. Review, update and conduct security training for personnel, based on roles.

4.8.2. Review the adequacy of physical and environmental controls.

4.8.3. Verify the encryption of Sensitive Data in transit.

4.8.4. Review access controls based on established roles and access profiles.

4.8.5. Update and review system administration documentation.

4.8.6. Update and review system maintenance policies.

4.8.7. Update and review system and integrity policies.

4.8.9. Review and implement updates to the System security plan.

4.8.10 Update risk assessment policies and procedures.

4.8.11 Update and implement incident response procedures.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

[redacted]

Appendix A – Compensating Controls to Security and Privacy Supplement

In the event that there is a security or privacy requirement outlined in this supplement that needs to be met by a compensating control, please identify it below and provide a proposed language change as well as a rationale for the change.

Reference	Current Language	Contractor's Proposed Change	Rationale of Proposed Change
Example: **Supplement 2 - Page 11**	**Example**: Provide vulnerability management services for the Contractor's internal secure network connection, including supporting remediation for identified vulnerabilities as agreed. As a minimum, the Contractor must provide vulnerability scan results to the State **monthly**.	**Example:** Provide vulnerability management services for the Contractor's internal secure network connection, including supporting remediation for identified vulnerabilities as agreed. As a minimum, the Contractor must provide vulnerability scan results to the State **weekly**.	Per company policy vulnerability report are only provided to customers on a quarterly basis.

JFS-DAS Security Supplement Addendum

In accordance with the Governor DeWine's executive order 2019-15D:

https://governor.ohio.gov/wps/portal/gov/governor/media/executive-orders/2019-15d

ODJFS is required to participate in the InnovateOhio Platform.

IOP - Identity & Access Management

The InnovateOhio Platform (IOP) provides a secure digital identity experience including an intuitive and interactive user experience for Ohio's citizens, businesses, and employees. The program provides centralized administration and synchronization of user identities to enable user provisioning and de-provisioning of identity and access for state systems. The *Application or Service* must, for all State/County employees, Businesses (Providers), and Citizens, provide single sign-on capabilities through integration with the State's Enterprise Identity Management system called Innovate Ohio Platform (IOP) leveraging IBM's Identity Federation.

IOP is aligned around four distinct pillars that support a consistent user experience for State of Ohio services constituents:

Enterprise Identity Pillar: Enterprise ID Management Framework having the following capabilities:

- User Provisioning
- Single Sign-on
- Identity Proofing
- 2-Factor Authentication (2FA)
- Federation
- Logging and Monitoring

Fraud and Risk Analytics Pillar: A comprehensive, risk-focused fraud detection and analytics service that can detect, prevent, analyze, and report on fraudulent activities in real time.

This enterprise, thin-layer tool is built upon the Federal Data Science Framework and provides:

- Continuous Machine Learning
- Scalable and Accessible Big Data
- Real-time Detection
- Key Graphics

User Experience Pillar: The User Experience Pillar supports an enhanced user and agency experience through consistent look and feel, optimized flows and functionalities and reduced redundancy.

- **User Interface:** (To the extent possible) standardized look and feel, navigation, and presentation of web sites, portals, and applications using a standard digital interface.
- **User Experience:** User-centric design, processes, tasks, and functions that support quicker, easier, and more secure access to and interaction with state agencies.
- **Agency Experience:** State-wide, centralized access point that adheres to the desired user experience and user interface, supported by standard tools, methods, and digital tool kits.

Platform and Portal Services Pillar: Provide an experience that promotes privacy, choice, and flexibility for citizens, businesses, and employees by:

- Enabling better, more secure access to an ever-growing set of digital services and self-help features across the state through a single proofed identity
- Enabling the state as an organization to consolidate historical transactions and cross-program / agency data to lead a better user experience

Required Interfaces with IOP:

For all Applications and Services that require authentication and/or authorizations:

Federated Single Sign-on: Application must support federated single sign-on using SAML 2.0 OR using Open ID Connect (OIDC) for identity assertion to authenticate the user to the Application

Authorization-Based Assertion Attributes: Application, optionally but preferred, would support Token assertions to determine appropriate authorizations (roles/permissions) for the individual, upon sign-in, based upon supplied Group membership attribute(s) (or other attributes as needed).

Automation of Provisioning / de-provisioning: Application, optionally but preferred, must support either:

1. A connector that is available within the IBM Identity suite, out of the box, to automate Agency user provisioning and de-provisioning tasks.
2. The Application has SOAP or REST Service(s) available that the IBM Identity suite (ISIM) can call to automatically perform provisioning and de-provisioning tasks.

Provisioning Tasks available:

- Create, or associate, an identity in the application for authentication and single sign-on (e.g. Just in Time provisioning or achieved through Group to role inspection above).
- Assign and Change an identity's assignment to specific Roles/Permissions within the application for authorization (or achieved through Group to role inspection above).

De-provisioning Tasks available:

- Delete, or un-associate, an identity in the application to revoke the person's ability to authenticate (or achieved through Group to role inspection above).
- Remove or alter specific Roles/Permissions per identity within the application to remove authorization (or achieved through Group to role inspection above).

Device Authentication: Tracking device information (IP Address, OS, etc.) is required by the application. Application, optionally but preferred, would support device authentication in conjuncture with the IOP Framework above. This will support the ability to prompt for additional security validation /authentication to user in the event the device is not recognized. Such as prompting for two-factor authentication, or having the user submit to ID Proofing, or challenge response questions for additional identity validation. Once the device is identified and tied to User identity, these questions can optionally not be presented or can periodically be reaffirmed based on business requirements.

[redacted]

IOP – Data Analytics

All Applications must make data available to the InnovateOhio Platform for secure, resilient Data Storage, reporting, analytics and data sharing across all Cabinet Agencies, Boards, and Commissions.

In summary, ODJFS is to: (1) Make data available to the InnovateOhio Platform for storage (staging before sharing) upon request of InnovateOhio; and (2) Share data pursuant to ORC 125.32 and at the direction of InnovateOhio, acknowledging any Federal restrictions or privacy requirements.

A standing Data Sharing Protocol outlines procedures and responsibilities of DAS and agencies for use of the InnovateOhio Platform under authority of ORC 125.32 and Executive Order 2019-15D.

DAS manages the InnovateOhio Platform which consists of a set of advanced data and analytics computing technologies including a robust data governance, security and privacy protection foundation to enable usage of state data and to protect data maintained on the platform. Note that a distinction must be made between 1) an agency providing and hosting data on the platform and 2) an agency approving the use of data for analysis. When an agency provides and hosts data on the InnovateOhio Platform, the agency is not granting “use” of the data to any party including DAS. DAS’s responsibility is to manage the platform as described within this protocol under and pursuant to ORC 125.18 and ORC 125.32. DAS is not given permission to “use” agency data unless the owning agency specifically approves.

ORC 125.32 states that, “A state agency that provides data under the program retains ownership over the data. Notwithstanding any other provision of the Revised Code, only the state agency that provides data under the program may be required under the law of this state to respond to requests for records or information regarding the provided data, including public records requests, subpoenas, warrants, and investigatory requests.”

Encryption

Personally identifiable information (PII), or confidential personal information (CPI - as defined in Ohio Revised Code 1347), as used in information security and privacy laws, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. One of the key security controls to protecting PII/CPI is Encryption. Encryption is to be utilized for PII/CPI data on all three states of existence:

Data at Rest: Data at Rest refers to inactive data which is stored physically in any digital form. This refers to both Structured (databases) and unstructured Data (files).

PII/CPI Data at Rest must be protected in one of the following methods:

- Encrypt the Entire Database with Transparent Data Encryption (TDE)
- Table/ Column or Field Level Encryption can be used within the Database Tables to encrypt just the PII/CPI

Ensure that any temporary representations (temp files or folders/ exports/ backups / reports, etc.) of PII/CPI is encrypted in that current state.

  - Applying newer encryption technologies and techniques, such as “homomorphic encryption” can be used to meet this requirement.

Encryption methods must use compliant NIST FIPS 140-2 Encryption Algorithms.

Data in Motion: Data in Motion refers to data which is being transferred across some network or transmission media.

PII/CPI Data in Motion must be protected in one of the following methods:

- Encrypt the Entire transmission using HTTPS or IPSEC (or equivalent protocols) between all devices and tiers (such as UI > APP > DB Tiers)
- Encrypt the PII/CPI data only in transmission (Example: SOAP message using WS-Security)

Encryption methods must use compliant NIST FIPS 140-2 Encryption Algorithms / Modules. When using the Transport Layer Security (TLS), TLS version 1.2 or higher must be used.

Data in Use: Data in Use refers to data actively being used across the network or temporarily residing in memory, or any data not currently “inactive”.

PII/CPI Data in Use must be protected in the following methods:

- Implement Memory protections, at a minimum, of Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) within Hardware and/or Software.
- Sessions must be unique to each authenticated user and be protected in way that meets the Open Web Application Security Project (OWASP)’s Application Security Verification Standard (ASVS).
- Application will use per user or session indirect object references where possible. All direct object References, from an untrusted source, must include an access control check to ensure the user is authorized for the requested object.
- Ensure that authentication /authorization checks are performed at each object at the controller and business logic levels, and not just at the presentation layer.
- Prevent Injection attacks by using a parameterized API or escape special characters using the specific escape syntax for that interpreter. Also, in addition, positive or “white list” input validation must be used.
- Device configurations must confirm to industry best practices for hardening (CIS Benchmarks).

- Components, such as libraries, frameworks, or other software modules used in development must be identified and a list provided to ODJFS at the conclusion of the project. A supported version of these components must be used at time of the contract.
- Autocomplete must be disabled on forms collecting PII/CPI, and caching must be disabled for pages that contain PII/CPI.
- Avoid the use of redirects and forwards as much as possible. When used, any such destination parameters must be a mapped value, and that server-side code translates this mapping to the target URL.

Audit Logging

A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network. Many logs within an organization contain records related to computer security. These computer security logs are generated by many sources, including security software, such as antivirus software, firewalls, and intrusion detection and prevention systems; operating systems on servers, workstations, and networking equipment; and applications.

The number, volume, and variety of computer security logs have increased greatly, which has created the need for computer security log management—the process for generating, transmitting, storing, analyzing, and disposing of computer security log data. Log management is essential to ensuring that computer security records are stored in sufficient detail for an appropriate period of time. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Logs are also useful when performing auditing and forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends and long-term problems. (Source NIST SP 800-92 "Guide to Computer Security Log Management")

ODJFS is required, for compliance to Federal and State Laws, codes, standards, and guidelines, to perform audit logging and management of those logs for its information systems.

Logging Requirements

The following Application Events must be record in the audit log(s) for the Information System.

Required Audit Events:

1. User account management activities (user creation, deletion, modification),

2. Application shutdown,
3. Application restart,
4. Application errors,
5. Failed and successful log-on(s),
6. Security policy modifications,
7. Use of administrator privileges,
8. All changes to logical access control authorities (e.g., rights, permissions, role assignment),
9. All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services,
10. Access to Personally Identifiable Information (PII – Also known as Confidential Personal Information (CPI) by Ohio Law),
11. Modification to Personally Identifiable Information (PII) - Also known as Confidential Personal Information (CPI)by Ohio Law),
12. File creation, deletion, or modification by the application (PDF, CSV, etc. - if Applicable).

Minimum Logging Requirements for Each Event

The following are the minimum required details that must be captured with each recorded event:

1. Identity of any user/subjects associated with the event (Who – user/group/device/system),
2. Event Information (What happened),
3. What Time the event occurred (When),
4. Subsystem or application the event occurred in (Where),
5. And the success/failure of the event (if applicable).

[redacted]

Audit Record Generation Services

All Applications, in the event of audit log processing failure (the application is unable to write to the security log/ log service) shall:

1. Notify appropriate personnel of the audit log processing failure, and
2. shall either:
   a. Stop all processing of further request s until the audit log processing is restored, or
   b. Queue all audit events to disk, until such time as the audit log processing is restored or the storage allocation is filled.

If storage allocation is full, the application shall stop all processing of all further requests until the audit log processing is restored.

[redacted]

Audit Retention, Aggregation, and Analysis

Applications are required to send the Audit Event Log information, through standard processes (such as SYSLOG) or through add-ons, to the Agencies Enterprise Log Management (ELM) Tool – Splunk and Enterprise Security Information and Event Management (SIEM) – QRadar.

Any required third-party tools or services to achieve this requirement, the vendor must acquire, purchase, and setup.

Audit Log information must be sent security to ODJFS ELM and/or SIEM tools and CPI Log repository (when applicable), using encryption methods that use compliant NIST FIPS 140-2 Encryption Algorithms / Modules.

[redacted]

Development Security

Data Set used in Development

All Data sets used in non-production environments (Development, Quality Testing, User Acceptance testing, etc.) must be generated or masked data or data sets (not real production data). Except, where approved by Agency Security Official, and using the same set of security controls that are in place for the non-production environment as the production environment. Masked or generated data or data sets can be generated by ODJFS for these purposes.

DevOps Vulnerability Scanning

Applications being developed for hosting by the state (on-premise) must adhere to ODJFS DevOps pipeline AppSec tools and processes. This includes both Static (code or white-box scanning) and Dynamic (application or black-box scanning) vulnerability scanning. Additionally,

any libraries or components used in the solution must be free of known critical or severe vulnerabilities and be scanned/evaluated by the ODJFS Software Composition Analysis (SCA) tool.

Hosted Solutions or Software as a Service (SaaS) Applications or Services. The vendor must provide proof that these scans are being performed and evaluated internally as part of their SDLC/DevOps processes, or by third Party compliance assessment certification/attestation (FedRAMP, ISO 27001, OWASP ASVS, CSA STAR, etc.).

Acceptance of uFACTS SOW General Terms and Conditions

April 13, 2020

DELOITTE RESPONSE

Deloitte has read, understands and agrees to the General Terms and Conditions contained herein.

THIS PAGE INTENTIONALLY LEFT BLANK.

PUA SOW GENERAL TERMS AND CONDITIONS

Statement of Work. The selected offeror's (the "Contractor") negotiated uFACTS SOW response, accepted uFACTS General Terms and Conditions, and the Cloud Services Agreement for uFACTS for PUA/DUA (collectively, the "SOW Documents") are a part of this Contract and describe the work (the "Project") the Contractor must do and any materials the Contractor must deliver (the "Deliverables") under this Contract with the Ohio Department of Job and Family Services (the "State"). The Contractor must do the Project in a professional, timely, and efficient manner and must provide the Deliverables in a proper fashion. The Contractor also must furnish its own support staff necessary for the performance of the Project in accordance with this Contract.

The Contractor must consult with the appropriate State representatives and others necessary to ensure a thorough understanding of the Project and performance of the Project in accordance with this Contract. The State may give instructions to or make requests of the Contractor relating to the Project, and the Contractor must comply with those instructions and fulfill those requests in a timely and professional manner. Those instructions and requests will be for the sole purpose of ensuring completion of the Project in accordance with this Contract and will not amend or alter the scope of the Project.

Term. Unless this Contract is terminated or expires without renewal, it will remain in effect until the Project is completed in accordance with this Contract, including all optional renewal periods for maintenance or continuing commitments, and the Contractor is paid. However, the current General Assembly cannot commit a future General Assembly to an expenditure. Therefore, this Contract will automatically expire June 30, 2021. If there is a State need beyond June 30, 2021, the State may renew this Contract in one (1) year term increments, subject to mutual agreement on scope and pricing and contingent on the discretionary decision of the Ohio General Assembly to appropriate funds for this Contract in each new biennium. Termination or expiration of this Contract will not limit the Contractor's continuing obligations with respect to Deliverables that the State paid for before or after termination or limit the State's rights in such.

The State's funds are contingent upon the availability of lawful appropriations by the Ohio General Assembly. If the General Assembly fails to continue funding for the payments and other obligations due as part of this Contract, the State's obligations under this Contract will terminate as of the date that the funding expires without further obligation of the State.

The Project has a completion date that is identified in the SOW Documents. The SOW Documents also may have several dates for the delivery of Deliverables or reaching certain milestones in the Project. The Contractor must make those deliveries, meet those milestones, and complete the Project within the times the SOW Documents require. If the Contractor does not meet those dates, the Contractor will be in default, and the State may terminate this Contract under the termination provision contained below.

The State also may have certain obligations to meet. Those obligations, if any, are also listed in the SOW Documents. If the State agrees that the Contractor's failure to meet the delivery, milestone, or completion dates in the SOW Documents is due to the State's failure to meet its own obligations in a timely fashion, then the Contractor will not be in default, and the delivery, milestone, and completion dates affected by the State's failure to perform will be extended by the same amount of time as the State's delay. The State will not unreasonably withhold such agreement, including if the Contractor provides substantiation of the facts. The Contractor may not rely on this provision unless the Contractor has in good faith exerted reasonable management skill to avoid an extension and has given the State meaningful written notice of the State's failure to meet its obligations within five business days of the Contractor's realization that the State's delay will or is likely to impact the Project. The Contractor must deliver any such notice (which may be via email or a project status report) to both the Project Representative and Procurement Representative and title the notice as a "Notice of State Delay." The notice must identify any delay in detail, as well as the impact the delay has or will have on the Project. Unless the State agrees (again not to be unreasonably withheld) that an equitable adjustment in the Contractor's Fee is warranted in the case of an extended delay, an extension of the Contractor's time to perform will be the Contractor's exclusive remedy for the State's delay. Should the State agree that an

equitable adjustment in the Contractor's Fee is warranted, the equitable adjustment will be handled as a Change Order under the Changes Section of this Contract, and the extension of time and equitable adjustment will be the exclusive remedies of the Contractor for the State's delay. The State will not unduly delay the execution of a Change Order that Contractor is entitled to under this provision.

The State seeks a complete project, and the Contractor must provide any incidental items omitted in the SOW Documents as part of the Contractor's not-to-exceed fixed price. The Contractor also must fully identify, describe, and document all systems that are delivered as a part of the Project. Unless expressly excluded elsewhere in the Contract, all hardware, software, supplies, and other required components (such as documentation, conversion, training, and maintenance) necessary for the Project to be complete and useful to the State are included in the Project and the not-to-exceed fixed price.

Compensation. In consideration of the Contractor's promises and State accepted performance, the State will pay the Contractor the amount(s) identified in the SOW Documents (the "Fee"), plus any other expenses identified as reimbursable in the SOW Documents. In no event, however, will payments under this Contract exceed the "total not-to-exceed" amount in the SOW Documents without the prior, written approval of the State and, when required, the Ohio Controlling Board and any other source of funding. The Contractor's right to the Fee is contingent on the complete and State accepted performance of the Project or, in the case of milestone payments or periodic payments of an hourly, daily, weekly, monthly, or annual rate, all relevant parts of the Project tied to the applicable milestone or period. Payment of the Fee also is contingent on the Contractor delivering a proper invoice and any other documents the SOW Documents require. An invoice must comply with the State's then current policies regarding invoices and their submission. The State will notify the Contractor in writing within 15 business days after it receives a defective invoice of any defect and provide the information necessary to correct the defect.

The Contractor must send all invoices under this Contract to the "bill to" address in the SOW Documents or in the applicable purchase order.

The State will pay the Contractor interest on any late payment, as provided in Section 126.30 of the Ohio Revised Code (the "Revised Code"). If the State disputes a payment for anything covered by an invoice, within 15 business days after receipt of that invoice, the State will notify the Contractor, in writing, stating the grounds for the dispute. The State then may deduct the disputed amount from its payment as a nonexclusive remedy. If the Contractor has committed a material breach, in the sole opinion of the State, the State also may withhold payment otherwise due to the Contractor on amounts disputed in good faith. Both parties will attempt to resolve any claims of material breach or payment disputes through discussions among the Contractor's Implementation Manager (e.g., Contractor's Project Manager), the Contractor's Project executive, the State's Project Representative, and the State Contract Management Administrator. The State will consult with the Contractor as early as reasonably possible about the nature of the claim or dispute and the amount of payment affected. When the Contractor has resolved the matter, then provided the resolution is not disputed by the State, the State will pay the withheld disputed amount within 30 business days after the matter is resolved. The State has no obligation to make any disputed payments until the matter is resolved, and the Contractor must continue its performance under this Contract pending resolution of the dispute or claim.

If the State has already paid the Contractor on an invoice but later disputes the amount covered by the invoice, and if the Contractor fails to correct the problem within 30 calendar days after written notice, the Contractor must reimburse the State for that amount at the end of the 30 calendar days as a nonexclusive remedy for the State. On written request from the Contractor, the State will provide reasonable assistance in determining the nature of the problem by giving the Contractor reasonable access to the State's facilities and any information the State has regarding the problem.

Payment of an invoice by the State will not prejudice the State's right to object to or question that or any other invoice or matter in relation thereto. The Contractor's invoice will be subject to reduction for amounts included in any invoice or payment made which are determined by the State not to constitute allowable costs, on the basis of audits conducted in accordance with the terms of this Contract. At the

State's sole discretion all payments shall be subject to reduction for amounts equal to prior overpayments to the Contractor.

That portion of the not-to-exceed fixed price identified in the SOW documents as being for a license to Contractor's proprietary uFACTS cloud hosted application will be paid in accordance with the Cloud Services Agreement between the parties governing such application.

Reimbursable Expenses. The State will pay all reimbursable expenses identified in the SOW Documents, if any, in accordance with the terms in the SOW Documents and, where applicable, Section 126.31 of the Revised Code. The Contractor must assume all expenses that it incurs in the performance of this Contract that are not identified as reimbursable in the SOW Documents.

In making any reimbursable expenditure, the Contractor always must comply with the more restrictive of its own, then current internal policies for making such expenditures or the State's then current policies. All reimbursable travel will require the advance written approval of the State's Project Representative. The Contractor must bill all reimbursable expenses monthly, and the State will reimburse the Contractor for them within 30 business days of receiving the Contractor's invoice.

Right of Offset. The State may set off the amount of any Ohio tax liability, liquidated damages or other damages from finally judicially awarded claims or settlement agreements or other obligation of the Contractor or its subsidiaries to the State, including any amounts the Contractor owes to the State under this or other contracts, against any payments due from the State to the Contractor under this or any other contracts with the State.

Certification of Funds. None of the rights, duties, or obligations in this Contract will be binding on the State, and the Contractor will not begin its performance until all the following conditions have been met:

(a) All statutory provisions under the Revised Code, including Section 126.07, have been met;
(b) All necessary funds are made available by the appropriate State entities;
(c) If required, the Controlling Board of Ohio approves this Contract; and
(d) If the State is relying on federal or third-party funds for this Contract, the State gives the Contractor written notice that such funds are available.

Employment Taxes. All people furnished by the Contractor (the "Contractor Personnel") are employees or subcontractors of the Contractor, and none are or will be deemed employees or contractors of the State. No Contractor Personnel will be entitled to participate in, claim benefits under, or become an "eligible employee" for purposes of any employee benefit plan of the State by reason of any work done under this Contract. The Contractor will pay all federal, state, local, and other applicable payroll taxes and make the required contributions, withholdings, and deductions imposed or assessed under any provision of any law and measured by wages, salaries, or other remuneration paid by or which may be due from the Contractor to the Contractor Personnel. The Contractor will indemnify, defend (with the consent and approval of the Ohio Attorney General), and hold the State harmless from and against all claims, losses, liability, demands, fines, and expense (including court costs, defense costs, and redeemable attorney fees) arising out of or relating to such taxes, withholdings, deductions, and contributions with respect to the Contractor Personnel. The Contractor's indemnity and defense obligations also apply to any claim or assertion of tax liability made by or on behalf of any Contractor Personnel or governmental agency on the basis that any Contractor Personnel are employees or contractors of the State, that the State is the "joint employer" or "co-employer" of any Contractor Personnel, or that any Contractor Personnel are entitled to any employee benefit offered only to eligible regular fulltime or regular part-time employees of the State.

Sales, Use, Excise, and Property Taxes. The State is exempt from any sales, use, excise, and property tax. To the extent sales, use, excise, or any similar tax is imposed on the Contractor in connection with the Project, such will be the sole and exclusive responsibility of the Contractor. Further, the Contractor will pay such taxes, together with any interest and penalties not disputed with the

appropriate taxing authority, whether they are imposed at the time the services are rendered or a later time.

PART TWO: WORK AND CONTRACT ADMINISTRATION

Related Contracts. The Contractor warrants that the Contractor has not and will not enter into any contracts without written approval of the State to perform substantially identical services for the State, such that the Project duplicates the work done or to be done under the other State contracts.

Other Contractors. The State may hold other contracts for additional or related work, including among others independent verification and validation (IV&V) work for this Project. The Contractor must fully cooperate with all other contractors and State employees and coordinate its work with such other contractors and State employees as may be required for the smooth and efficient operation of all related or additional work. The Contractor may not act in any way that may unreasonably interfere with the work of any other contractors or the State's employees. Further, the Contractor must fully cooperate with any IV&V contractor assigned to this Project. Such cooperation includes expeditiously providing the IV&V contractor with full and complete access to all project work product, records, materials, personnel, meetings, and correspondence of Contractor or subcontractor with the State or its other vendors regarding the project as the IV&V contractor may request. If the State assigns an IV&V contractor to the Project, the State will obligate the IV&V contractor to a confidentiality provision similar to the Confidentiality Section contained in this Contract. Additionally, the Contractor must include the obligations of this provision in all its contracts with its subcontractors that work on this project.

Subcontracting. The Contractor may not enter into subcontracts related to the Project after award without written approval from the State. Nevertheless, the Contractor will not need the State's written approval to subcontract for the purchase of commercial goods that are required for satisfactory completion of the Project. All subcontracts will be at the sole expense of the Contractor unless expressly stated otherwise in the SOW Documents.

The State's approval of the use of subcontractors does not mean that the State will pay for them. The Contractor will be solely responsible for payment of its subcontractor and any claims of subcontractors for any failure of the Contractor or any of its other subcontractors to meet the performance schedule or performance specifications for the Project in a timely and professional manner. The Contractor must hold the State harmless for and must indemnify the State against any such claims.

The Contractor assumes responsibility for all Deliverables whether it, a subcontractor, or third-party manufacturer produces them in whole or in part. Further, the Contractor will be the sole point of contact with regard to contractual matters, including payment of all charges resulting from the Contract. Further, the Contractor will be fully responsible for any default by a subcontractor, just as if the Contractor itself had defaulted.

If the Contractor uses any subcontractors, each subcontractor must have a written agreement with the Contractor. That written agreement must incorporate this Contract by reference. The agreement also must pass through to the subcontractor all provisions of this Contract that would be fully effective only if they bind both the subcontractor and the Contractor. Among such provisions are the limitations on the Contractor's remedies, the insurance requirements, record keeping obligations, and audit rights. Some sections of this Contract may limit the need to pass through their requirements to subcontracts to avoid placing cumbersome obligations on minor subcontractors. This exception is applicable only to sections that expressly provide an exclusion for small-dollar subcontracts. Should the Contractor fail to pass through any provisions of this Contract to one of its subcontractors and the failure damages the State in any way, the Contractor must indemnify the State for the damage.

Record Keeping. The Contractor must keep all financial records in accordance with generally accepted accounting principles or equivalent consistently applied. The Contractor also must file documentation to support each action under this Contract in a manner allowing the documentation to be readily located. Additionally, the Contractor must keep all Project-related records and documents at its principal place of business or at its office where the work was performed.

Audits. During the term of this Contract and for three years after the payment of the Contractor's Fee, on reasonable notice, and during customary business hours, the State may audit the Contractor's records and other materials that relate to the Project. This audit right also applies to the State's duly authorized representatives and any person or organization providing financial support for the Project. State audit rights will apply to those Contractor materials that are required to verify the accuracy of a Contractor invoice to the State inclusive of: Contractor personnel timesheets; Contractor purchased or provided equipment for benefit of the State that will remain in the State's possession; State deliverable acceptance documentation; any required State written approvals as required herein; final Work products and deliverables; any partial or incomplete Work products or deliverables that should the Contractor submit for partial compensation from the State as a result of termination of this contract.

Right to Terminate as a Result of Audit Findings. In the event the State determines that the results of any examination of the Contractor is unsatisfactory per the requirements of the Contract and not remedied within a 30-day period following written notice from the State, the State may terminate this Agreement, in part or in full.

If the Contractor fails to satisfy the requirements of the State with regard to security of information, or if an examination reveals information that would result in a continuing contractual relationship that causes the State to be in violation of any law, the State may terminate this Contract immediately without notice.

Insurance. Contractor shall procure and maintain for the duration of the contract insurance against claims for injuries to persons or damages to property which may arise from or in connection with the performance of the work hereunder by the Contractor, its agents, representatives, or employees. Contractor shall procure and maintain for the duration of the contract insurance for claims arising out of their services and including, but not limited to loss, damage, theft or other misuse of data, infringement of intellectual property, invasion of privacy and breach of data.

MINIMUM SCOPE AND LIMIT OF INSURANCE

Coverage shall be at least as broad as:

1. Commercial General Liability (CGL): written on an "occurrence" basis, including products and completed operations, property damage, bodily injury and personal & advertising injury with limits no less than $1,000,000 per occurrence. If a general aggregate limit applies, either the general aggregate limit shall apply separately to this project/location or the general aggregate limit shall be twice the required occurrence limit. Defense costs shall be outside the policy limit.

2. Automobile Liability: covering Code 1 (any auto), or if Contractor has no owned autos, Code 8 (hired) and 9 (non-owned), with a limit no less than $1,000,000 per accident for bodily injury and property damage.

3. Workers' Compensation insurance as required by the State of Ohio, or the state in which the work will be performed, with Statutory Limits, and Employer's Liability Insurance with a limit of no less than $1,000,000 per accident for bodily injury, $1,000,000 per employee for bodily injury by disease and $1,000,000 policy limit for bodily injury by disease. If Contractor is a sole proprietor, partnership or has no statutory requirement for workers' compensation, Contractor must provide a letter stating that it is exempt and agreeing to hold Entity harmless from loss or liability for such.

4. Technology Professional Liability (Errors and Omissions) Insurance appropriate to the Contractor's profession, with limits not less than $2,000,000 per claim, $2,000,000 aggregate for legal liability arising out of or resulting from wrongful acts, errors omissions in negligence in performance of work under this Contract. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Contractor in this agreement and shall cover

Contractor personnel or subcontractors, as applicable, who perform professional services related to this agreement.

5. Cyber liability (first and third party) with limits not less than $2,000,000 per claim, $10,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Contractor in this agreement and shall include, but not be limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The coverage shall provide for breach response costs as well as regulatory fines and penalties and credit monitoring expenses with limits sufficient to respond to these obligations. The Cyber liability insurance is embedded in Contractor's Technology Professional Liability coverage form.

The Insurance obligations under this agreement shall be the minimum Insurance coverage requirements and/or limits shown in this agreement. Any insurance proceeds in excess of or broader than the minimum required coverage and/or minimum required limits, which are applicable to a given loss, shall be available for such loss. No representation is made that the minimum Insurance requirements of this agreement are sufficient to cover the obligations of the Contractor under this agreement.

The insurance policies are to contain, or be endorsed to contain, the following provisions:

Additional Insured Status
Except for Workers' Compensation and Professional Liability insurance (including Technology Liability and Cyber Liability), the State of Ohio, its officers, officials and employees are to be covered as additional insureds with respect to liability arising out of work performed by or on behalf of the Contractor including materials, parts, or equipment furnished in connection with such work. Coverage can be provided in the form of a blanket endorsement to the Contractor's insurance.

Primary Coverage
For any claims related to this contract, the Contractor's insurance coverage shall be primary insurance. Any insurance or self-insurance maintained by the State of Ohio, its officers, officials and employees shall be excess of the Contractor's insurance and shall not contribute with it.

Umbrella or Excess Insurance Policies
Umbrella or excess commercial liability policies may be used in combination with primary policies to satisfy the limit requirements above. Such Umbrella or excess commercial liability policies shall apply without any gaps in the limits of coverage and be at least as broad as and follow the form of the underlying primary coverage required above.

Notice of Cancellation
Contractor shall provide State of Ohio with 30 days written notice of cancellation or adverse material change to any insurance policy required above, except for non-payment cancellation, unless Contractor is able to obtain replacement insurance meeting all of the requirements and specifications herein without lapse, and provides the State with the replacement certifications. Adverse material change shall be defined as any change to the minimum insurance limits, terms or conditions that would limit or alter the State's available recovery under any of the policies required above. A lapse in any required insurance coverage during this Agreement shall be a breach of this Agreement.

Waiver of Subrogation
Contractor hereby grants to State of Ohio a waiver of any right to subrogation which any insurer of said Contractor may acquire against the State of Ohio by virtue of the payment of any loss under

such insurance unless prohibited by law. Contractor agrees to obtain any endorsement that may be necessary to affect this waiver of subrogation, but this provision applies regardless of whether or not the State of Ohio has received a waiver of subrogation endorsement from the insurer.

Deductibles and Self-Insured Retentions
Deductibles and self-insured retentions must be declared to and approved by the State. The State may require the Contractor to provide proof of ability to pay losses and related investigations, claims administration and defense expenses within the retention in the form of a financial stability statement.

Claims Made Policies
If any of the required policies provide coverage on a claims-made basis:

1. The Retroactive Date must be shown and must be before the date of the contract or the beginning of contract work.

2. Insurance must be maintained, and evidence of insurance must be provided for at least five (5) years after completion of the contract of work.

3. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a Retroactive Date prior to the contract effective date, the Contractor must purchase "extended reporting" coverage for a minimum of five (5) years after completion of contract work. The Discovery Period must be active during the Extended Reporting Period for wrongful acts committed prior to such cancellation or non-renewal.

Verification of Coverage
Contractor shall furnish the State of Ohio with original industry standard Acord certificates and amendatory endorsements for waiver of subrogation and blanket additional insured effecting coverage required by this clause. All certificates and endorsements are to be received and approved bythe State of Ohio before work commences. However, failure to obtain the required documents prior to the work beginning shall not waive the Contractor’s obligation to provide them. The State of Ohio reserves the right to require the identified endorsements required by these specifications, at any time.

Subcontractors
Contractor shall require and verify that all subcontractors maintain insurance meeting all the requirements stated herein, and Contractor shall ensure that State of Ohio is an additional insured on applicable insurance required from subcontractors.

Special Risks or Circumstances
State of Ohio reserves the right to modify these requirements with reasonable advance written notice, including limits, based on the nature of the risk, prior experience, insurer, coverage, or other special circumstances.

Replacement Personnel. If the SOW Documents contain the names of specific people identified as Key Project Persons who will work on the Project, then the quality and professional credentials of those people were material factors in the State's decision to enter into this Contract. Therefore, the Contractor must use all commercially reasonable efforts to ensure the continued availability of those people. Also, the Contractor may not remove those people from the Project for the duration of their role as reflected in the then-current project plan without the prior written consent of the State, except as provided below.

The Contractor may remove a Key Project Person listed in the SOW Documents from the Project, if doing so is necessary for legal or disciplinary reasons, or in the case of the person’s resignation of the ceasing of his or her employment with the Contractor or in the case of a leave of absence due to medical or personal extenuating circumstances. However, the Contractor must make a reasonable effort to give the

State 30 calendar days' prior written notice of the removal if circumstances allow or if not, as much notice as is reasonably possible.

If the Contractor removes a Key Project Person listed in the SOW Documents from the Project for any reason other than those specified above, the State may assess liquidated damages in the amount of
$1,800.00 for every day between the date on which the individual was removed and the date that this Contract is terminated or the individual's qualified replacement, selected in accordance with the process identified in this section, starts performing on the Project. The State also may provide the Contractor with written notice of its default under this section, which the Contractor must cure within 30 days. Should the Contractor fail to cure its default within the 30-day cure period, this Contract may be terminated immediately for cause, and the State will be entitled to damages in accordance with the Suspension and Termination Section of this Contract due to the termination. Should the State assess liquidated damages or otherwise be entitled to damages under this provision, it may offset these damages from any Fees due under this Contract.

The Contractor must have qualified replacement people available to replace any people listed in the SOW Documents by name and identified as a Key Project Person. When the removal of a listed Key Project Person is permitted under this Section, or if such a person becomes unavailable, the Contractor must submit the resumes for two replacement people to the State for each Key Project Person removed or who otherwise becomes unavailable. The Contractor must submit the two resumes, along with such other information as the State may reasonably request, within five business days after the decision to remove a Key Project Person is made or the unavailability of a listed Key Project Person becomes known to the Contractor.

The State will select one of the two proposed replacements or will reject both of them within ten business days after the Contractor has submitted the proposed replacements to the State. The State may reject the proposed replacements for any legal reason. Should the State reject both replacement candidates due to their failure to meet the minimum qualifications identified in the SOW Documents, or should the Contractor fail to provide the notice required under this Section or fail to provide two qualified replacement candidates for each removed or unavailable Key Project Person, the Contractor will be in default and the cure period for default specified elsewhere in this Contract will not apply. In any such case, the State will have the following options:

(a) The State may assess liquidated damages in the amount of $1,800.00 for every day between the date on which the Contractor failed to provide the applicable notice, failed to provide the two replacement candidates, or the date the State rejected all candidates for cause and the date on which the Contractor affects a cure or the Contract expires without renewal or is terminated.
(b) The State may terminate this Contract immediately for cause and without any cure period.

Should the State exercise its option under item (a) above, it nevertheless will be entitled anytime thereafter to exercise its option under item (b) above. Additionally, should the State terminate this Contract under this provision, it will be entitled to damages in accordance with the Suspension and Termination Section of this Contract due to the termination. Should the State assess liquidated damages or otherwise be entitled to damages under this provision, it may offset these damages from any Fees due under this Contract.

The State may determine that the proposed replacement candidates meet the minimum qualifications of this Contract and still substantially reduce the value the State perceived it would receive through the effort of the original individual(s) the Contractor proposed and on whose credentials the State decided to enter into this Contract. Therefore, the State will have the right to reject any candidate that the State determines may provide it with diminished value.

Should the State reject both proposed candidates for any legal reason other than their failure to meet the minimum qualifications identified in the SOW Documents, the State may terminate this Contract for its convenience.

The State has an interest in providing a healthy and safe environment for its employees and guests at its facilities. The State also has an interest in ensuring that its operations are carried out in an efficient, professional, legal, and secure manner. Therefore, the State will have the right to require the Contractor to remove any individual involved in the Project, if the State determines that any such individual has or may interfere with the State's interests identified above. In such a case, the request for removal will be treated as a case in which an individual providing services under this Contract has become unavailable, and the Contractor must follow the procedures identified above for replacing unavailable Key Project Persons. This provision also applies to people that the Contractor's subcontractors engage, if they are listed by name as a Key Project Person in the SOW Documents.

Suspension and Termination. The State may terminate this Contract in full or in part for cause if the Contractor defaults in meeting its obligations under this Contract and fails to cure its default within the time allowed by this Contract, or if a petition in bankruptcy (or similar proceeding) has been filed by or against the Contractor. The State also may terminate this Contract if the Contractor violates any law or regulation in doing the Project, or if it reasonably appears to the State that the Contractor's performance is substantially endangered through no fault of the State. In any such case, the termination will be for cause, and the State's rights and remedies will be those identified below for termination for cause.

On written notice, the Contractor will have 30 calendar days to cure any breach of its obligations under this Contract or the substantial endangerment of performance as referenced above, provided the breach is curable. If the Contractor fails to cure the breach within 30 calendar days after written notice, or if the breach/endangerment is not one that is curable, the State will have the right to terminate this Contract immediately on notice to the Contractor. The State also may terminate this Contract in the case of breaches that are cured within 30 calendar days but are persistent. "Persistent" in this context means that the State has notified the Contractor in writing of the Contractor's failure to meet any of its obligations three times. After the third notice, the State may terminate this Contract on written notice to the Contractor without a cure period if the Contractor again fails to meet any obligation. The three notices do not have to relate to the same obligation or type of failure. Some provisions of this Contract may provide for a shorter cure period than 30 calendar days or for no cure period at all, and those provisions will prevail over this one. If a particular section does not state what the cure period will be, this provision will govern.

The State also may terminate this Contract in full or in part for its convenience and without cause or if the Ohio General Assembly fails to appropriate funds for any part of the Project upon as much notice as is practicable, as afforded under the circumstances of the situation and as allowed by Ohio law. If a third party is providing funding for the Project, the State also may terminate this Contract should that third party fail to release any Project funds. The SOW Documents normally identify any third-party source of funds for the Project, but an absence of such in the SOW Documents will not diminish the State’s rights under this section.

The notice of termination, whether for cause or without cause, will be effective as soon as the Contractor receives it. As of the effective date of termination, the Contractor must immediately cease all work on the project and take all steps necessary to minimize any costs the Contractor will incur related to this Contract. The Contractor also must immediately prepare a report and deliver it to the State. The report must be all-inclusive and must detail the work completed at the date of termination, the percentage of the Project's completion, any costs incurred in doing the Project to that date, and any Deliverables completed or partially completed but not delivered to the State at the time of termination. The Contractor also must deliver all the completed and partially completed Deliverables to the State with its report. However, if the State determines that delivery in that manner would not be in its interest, then the State will designate a suitable alternative form of delivery, which the Contractor must honor.

If the State terminates this Contract for cause, the State will be entitled to cover for the Work by using another Contractor on such commercially reasonable terms as the State and the covering contractor may agree. In such case, the Contractor may be liable to the State for all costs paid to a substitute provider related to covering for the Work to the extent that such costs, when combined with payments already made to the Contractor for the Work before termination, exceed the costs that the State would have incurred under this Contract. The Contractor also may be liable for any other direct damages resulting from its breach of this Contract or other fault of Contractor leading to termination for cause. If the Contractor fails to deliver Deliverables or provide services in accordance with this Contract, the State has the right to withhold any and all payments due to the Contractor for such Deliverables or services without penalty or work stoppage by the Contractor until such failure to perform is cured.

If the termination is for the convenience of the State, then except with respect to any amounts disputed in good faith by the State, the Contractor will be entitled to the Contract price as prorated for deliverables, products or services in accordance with the report required above and not previously paid for provided in that in no event will total payments exceed the amount payable to the Contractor as if the Contract had been fully performed. For items not specifically priced, the State will use fair market value to determine the price owed. The Contractor will use generally accepted accounting principles or equivalent and sound business practices in determining all costs claimed, agreed to, or determined under this clause.

The State will have the option of suspending this Contract in full or in part in accordance with the following paragraphs rather than terminating the Project, if the State believes that doing so would better serve its interests. In the event of a suspension for the convenience of the State, the Contractor will be entitled to receive payment for the work performed before the suspension. In the case of suspension of the Project for cause rather than termination for cause, the State must provide notice of intended suspension for cause, the State may suspend the Contract in accordance with this section and the Contractor will not be entitled to any compensation for any work performed during such suspension period; provided that where the breach/endangerment is curable, the State shall provide the Contractor with a minimum of a ten (10) business day cure period prior to any such suspension. If the State reinstates the Project after suspension for cause, rather than terminating this Contract after the suspension, the Contractor may be entitled to compensation for work performed before the suspension, less any damages for which Contractor is obligated to pay to the State resulting from the Contractor’s breach of this Contract or other fault giving rise to such suspension. Any amount due for work performed before a suspension for cause begins or after a suspension for cause ends will be offset by any damages for which Contractor is obligated to pay to the State from the default or other fault giving rise to the suspension.

In the case of a suspension for the State's convenience, the State will calculate the amount of compensation due to the Contractor for work performed before the suspension in the same manner as provided in this section for termination for the State's convenience. The Contractor will not be entitled to compensation for any other costs associated with a suspension for the State’s convenience, and the State will make no payment under this provision to the Contractor until the Contractor submits a proper invoice. If the State decides to allow the work to continue rather than terminating this Contract after the suspension, the State will not be required to make any payment to the Contractor other than those payments specified in this Contract and in accordance with the payment schedule specified in this Contract for properly completed work.

Any notice of suspension, whether with or without cause, will be effective immediately on the Contractor's receipt of the notice. The Contractor will prepare a report concerning the Project just as is required by this Section in the case of termination. After suspension of the Project, the Contractor may not perform any work without the consent of the State and may resume work only on five (5) days prior written notice from the State to do so; provided that the Contractor will not be in breach of this Contract if it needs to replace any personnel (including any Key Project Person) as a result of any suspension hereunder, where such replacement personnel shall be subject to State approval in accordance with the “Replacement Personnel” provision above. In any case of suspension, the State retains its right to terminate this Contract rather than to continue the suspension or resume the Project.

The State may not suspend the Project for its convenience more than twice during the term of this Contract, and any suspension for the State's convenience may not continue for more than 30 calendar days. If the Contractor does not receive notice to resume or terminate the Project within the 30-day suspension, then this Contract will terminate automatically for the State's convenience at the end of the 30-calendar day period.

Any default by the Contractor or one of its subcontractors will be treated as a default by the Contractor and all of its subcontractors. The Contractor will be solely responsible for satisfying any claims of its subcontractors for any suspension or termination and must indemnify the State for any liability to them. Notwithstanding the foregoing, each subcontractor must hold the State harmless for any damage caused to them from a suspension or termination. They must look solely to the Contractor for any compensation to which they may be entitled.

Representatives. The State's representative under this Contract will be the person identified in the SOW Documents or in a subsequent notice to the Contractor as the "Work Representative." The Work Representative will review all reports the Contractor makes in the performance of the Project, will conduct all liaison with the Contractor, and will accept or reject the Deliverables and the completed Project. The Project Representative may delegate his responsibilities for individual aspects of the Project to one or more managers, who may act as the Project Representative for those individual portions of the Project.

The Contractor's Implementation Manager under this Contract will be the person identified on the SOW Documents as the "Implementation Manager." The Implementation Manager will be the Contractor's liaison with the State under this Contract. The Implementation Manager also will conduct all Project meetings and prepare and submit to the Work Representative all reports, plans, and other materials that the SOW Documents require from the Contractor.

Either party, upon written notice to the other party, may designate another representative. However, the Contractor may not replace the Implementation Manager without the approval of the State if that person is identified in the SOW Documents by name or as a Key Project Person on the Project.

Project Responsibilities. The State will be responsible for providing only those things, if any, expressly identified in the SOW Documents. If the State has agreed to provide facilities or equipment, the Contractor, by signing this Contract, warrants that the Contractor has either inspected the facilities and equipment or has voluntarily waived an inspection and will work with the equipment and facilities on an "as is" basis.

The Contractor must assume the lead in the areas of management, design, and development of the Project. The Contractor must coordinate the successful execution of the Project and direct all Project activities on a day-to-day basis, with the advice and consent of the Project Representative. The Contractor will be responsible for all communications regarding the progress of the Project and will discuss with the Project Representative any issues, recommendations, and decisions related to the Project.

If any part of the Project requires installation on the State's property, the State will provide the Contractor with reasonable access to the installation site for the installation and any site preparation that is needed. After the installation is complete, the Contractor must complete an installation letter and secure the signature of the Project Representative certifying that installation is complete and the Project, or applicable portion of it, is operational. The letter must describe the nature, date, and location of the installation, as well as the date the Project Representative certified the installation as complete and operational.

Unless otherwise provided in the SOW Documents, the Contractor is solely responsible for obtaining all official permits, approvals, licenses, certifications, and similar authorizations required by any local, state, or federal agency for the Project and maintaining them throughout the duration of this Contract.

Changes. The State may make reasonable changes within the general scope of the Project. Upon mutual agreement with the Contractor, the State will do so by issuing a written order under this Contract describing the nature of the change ("Change Order"). Additionally, if the State provides directions or makes requests of the Contractor without a change order, and the Contractor reasonably believes the directions or requests are outside the specifications for the Project, the Contractor may request a Change Order from the State. The parties will handle such changes as follows: The Contractor will provide pricing to the State. The State will execute a Change Order once it and the Contractor have agreed on the description of and specifications for the change, as well as any equitable adjustments that need to be made in the Contractor's Fee or the performance schedule for the work. Then within five business days after receiving the Change Order, the Contractor must sign it to signify agreement with it.

If a change causes an increase in the cost of, or the time required for, the performance of the Project, the Contractor must notify the State in writing and request an equitable adjustment in its Fee, the delivery schedule, or both before the Contractor signs the Change Order. If the Contractor claims an adjustment under this section in connection with a change to the Project not described in a written Change Order, the Contractor must notify the State in writing of the claim within five business days after the Contractor receives a written change request from the State and before work on the change begins. Otherwise, the Contractor will have waived the claim. In no event will the State be responsible for any increase in the Fee or revision in any delivery schedule unless the State expressly ordered the relevant change in writing and the Contractor has complied with the requirements of this section. Provided the State has complied with the procedure for Change Orders in this section, nothing in this clause will excuse the Contractor from proceeding with performance of the Project, as changed.

Where an equitable adjustment to the Contractor's Fee is appropriate, the State and the Contractor may agree upon such an adjustment. If the State and the Contractor are unable to agree, either party may submit the dispute to the senior management of the Contractor and the senior management of the State's Department of Administrative Services for resolution. If within 30 calendar days following referral to senior management, the claim or dispute has not been resolved, the Contractor must submit its actual costs for materials needed for the change (or estimated amount if the precise amount of materials cannot be determined) and an estimate of the hours of labor required to do the work under the Change Order. The Contractor must break down the hours of labor by employee position and provide the actual hourly pay rate for each employee involved in the change. The total amount of the equitable adjustment for the Change Order then will be made based on the actual cost of materials (or estimated materials) and Contractor's then-current hourly rates for each person for their performance of the work required to do the change (based on the estimated hours of work required to do the change). This amount will be the not-to-exceed amount of the Change Order. If the change involves removing a requirement from the Project or replacing one part of the Project with the change, the State will get a credit for the work no longer required under the original scope of the Project. The credit will be calculated in the same manner as the Contractor's Fee for the change, and the not-to-exceed amount will be reduced by this credit.

The Contractor is responsible for coordinating changes with its subcontractors and adjusting their compensation and performance schedule. The State will not pay any subcontractor for the Change Order. If a subcontractor will perform any work under a Change Order, that work must be included in the Contractor's not-to-exceed amount and calculated in the same manner as the Contractor's equitable adjustment for the portion of the work the Contractor will perform. The Contractor will not receive an overhead percentage for any work a subcontractor will do under a Change Order.

If the SOW Documents provide for the retainage of a portion of the Contractor's Fee, all equitable adjustments for Change Orders also will be subject to the same retainage, which the State will pay only on completion and acceptance of the Project, as provided in the SOW Documents.

Excusable Delay. Neither party will be liable for any delay in its performance that arises from causes beyond its control and without its negligence or fault. The delayed party must notify the other promptly of any material delay in performance and must specify in writing the proposed revised performance date as soon as practicable after notice of delay. In the event of any such excusable delay, the date of

performance or of delivery will be extended for a period equal to the time lost by reason of the excusable delay. The delayed party also must describe the cause of the delay and what steps it is taking to remove the cause. The delayed party may not rely on a claim of excusable delay to avoid liability for a delay if the delayed party has not taken commercially reasonable steps to mitigate or avoid the delay. Things that are controllable by the Contractor's subcontractors will be considered controllable by the Contractor, except for third-party manufacturers supplying commercial items and over whom the Contractor has no legal control.

Independent Contractor Acknowledgement. It is fully understood and agreed that Contractor is an independent contractor and is not an agent, servant, or employee of the State of Ohio or the Ohio Department of Administrative Services. Contractor declares that it is engaged as an independent business and has complied with all applicable federal, state, and local laws regarding business permits and licenses of any kind, including but not limited to any insurance coverage, workers' compensation, or unemployment compensation that is required in the normal course of business and will assume all responsibility for any federal, state, municipal or other tax liabilities. Additionally, Contractor understands that as an independent contractor, it is not a public employee and is not entitled to contributions from DAS to any public employee retirement system.

Contractor acknowledges and agrees any individual providing personal services under this agreement is not a public employee for purposes of Chapter 145 of the Ohio Revised Code. Unless Contractor is a "business entity" as that term is defined in ORC. 145.037 ("an entity with five or more employees that is a corporation, association, firm, limited liability company, partnership, sole proprietorship, or other entity engaged in business") Contractor shall have any individual performing services under this agreement complete and submit to the ordering agency the Independent Contractor/Worker Acknowledgement found at the following link: https://www.opers.org/forms-archive/PEDACKN.pdf

Contractor's failure to complete and submit the Independent/Worker Acknowledgement prior to commencement of the work, service or deliverable, provided under this agreement, shall serve as Contractor's certification that contractor is a "Business entity" as the term is defined in ORC Section 145.037.

Publicity. The Contractor shall not do the following without prior, written consent from the State:

1. Advertise or publicize that the Contractor is doing business with the State;

Use this Contract as a marketing or sales tool; or

2. Affix any advertisement or endorsement, including any logo, graphic, text, sound, video, and company name, to any State-owned property, application, or website, including any website hosted by Contractor or a third party.

PART THREE: OWNERSHIP AND HANDLING OF INTELLECTUAL PROPERTY AND CONFIDENTIAL INFORMATION

Confidentiality. The State and Contractor may disclose to one another written material or oral or other information that the disclosing party treats as confidential ("Confidential Information"). Title to the Confidential Information and all related materials and documentation the State delivers to the Contractor will remain with the State. The receiving party must treat such Confidential Information as secret, if it is so marked, otherwise identified as such, or when, by its very nature, it deals with matters that, if generally known, would be damaging to the best interest of the public, other contractors, potential contractors with the State, or individuals or organizations about whom the State keeps information. By way of example, information must be treated as confidential if it includes any proprietary documentation, materials, flow charts, codes, software, computer instructions, techniques, models, information, diagrams, know-how, trade secrets, data, business records, security measures (both physical and computer), or marketing information. By way of further example, the receiving party also must treat as confidential materials such as police and investigative records, files containing personal information about individuals or employees of the State, such as personnel records, tax records, and so on, court and administrative records related to pending actions, any material to which an attorney-client, physician-patient, or similar privilege may apply, and any documents or records excluded by Ohio law from public records disclosure requirements. Nothing in this Confidentiality Section will prevent the State from disclosing public records as required under Ohio Revised Code Section 149.43.

The Contractor may not disclose any Confidential Information to third parties and must use it solely to do the Project. The Contractor must restrict circulation of Confidential Information within its organization and then only to people in the Contractor's organization that have a need to know the Confidential Information to do the Project. The Contractor will be liable for the disclosure of such information, whether the disclosure is intentional, negligent, or accidental, unless otherwise provided below.

The Contractor will not incorporate any portion of any Confidential Information into any work or product, other than a Deliverable, and will have no proprietary interest in any of the Confidential Information. Furthermore, the Contractor must cause all of its Personnel who have access to any Confidential Information to execute a confidentiality agreement incorporating the obligations in this section.

The Contractor's obligation to maintain the confidentiality of the Confidential Information will not apply where such: (1) was already in the Contractor's possession before disclosure by the State, and such was received by the Contractor without obligation of confidence; (2) is independently developed by the Contractor; (3) except as provided in the next paragraph, is or becomes publicly available without breach of this Contract; (4) is rightfully received by the Contractor from a third party without an obligation of confidence; (5) is disclosed by the Contractor with the written consent of the State; or (6) is released in accordance with a valid order of a court or governmental agency, provided that the Contractor (a) notifies the State of such order immediately upon receipt of the order and (b) makes a reasonable effort to obtain a protective order from the issuing court or agency limiting disclosure and use of the Confidential Information solely for the purposes intended to be served by the original order of production. The Contractor must return all originals of any Confidential Information and destroy any copies it has made on termination or expiration of this Contract.

Information that may be available publicly through other sources about people that is personal in nature, such as medical records, addresses, phone numbers, social security numbers, and similar things are nevertheless sensitive in nature and may not be disclosed or used in any manner except as expressly authorized in this Contract. Therefore, item (3) in the preceding paragraph does not apply, and the Contractor must treat such information as Confidential Information whether it is available elsewhere or not.

The Contractor may disclose Confidential Information to its subcontractors on a need-to-know basis, but the Contractor first must obligate them to the requirements of this section.

Confidentiality Agreements. When the Contractor performs services under this Contract that require the Contractor’s and its subcontractors’ personnel to access facilities, data, or systems that the State in its

sole discretion deems sensitive, the State may require the Contractor's and its subcontractors' personnel with such access to sign an individual confidential agreement and policy acknowledgements, and have a background check performed before accessing those facilities, data, or systems. Each State agency, board, and commission may require a different confidentiality agreement or acknowledgement, and the Contractor's and its subcontractors' personnel may be required to sign a different confidentiality agreement or acknowledgement for each agency. The Contractor must immediately replace any of its or its subcontractors' personnel who refuse to sign a required confidentiality agreement or acknowledgment or have a background check performed.

Ownership of Deliverables. The State owns all Deliverables that the Contractor produces under this Contract, including Deliverables comprised of software modifications and documentation, with all rights, title, and interest in all intellectual property that come into existence through the Contractor's custom work being assigned to the State. Additionally, the Contractor waives any author rights and similar retained interests in custom-developed material. The Contractor must provide the State with all assistance reasonably needed to vest such rights of ownership in the State. The Contractor will retain ownership of all tools, methods, techniques, standards, and other development procedures created by Contractor or its subcontractors prior to or outside of the Services, as well as generic and preexisting shells, subroutines, and similar material, and in each case any modifications and derivatives thereof, incorporated into any custom Deliverable ("Pre-existing Materials"), if the Contractor provides the non-exclusive license described in the next paragraph.

The Contractor may grant the State a worldwide, non-exclusive, royalty-free, perpetual license to use, modify, and distribute all Pre-existing Materials for State use that are incorporated into any custom-developed Deliverable rather than grant the State ownership of the Pre-existing Materials. The State may distribute such Pre-existing materials to third parties only to the extent required by governmental funding mandates. The Contractor may not include in any custom Deliverable any intellectual property unless such has been created under this Contract or qualifies as Pre-existing Material. If the Contractor wants to incorporate any Pre-existing Materials into a custom Deliverable and not provide to the State the license granted in this paragraph, the Contractor must first disclose that desire to the State in writing and seek the State's approval for doing so in advance. The State will not be obligated to provide that approval, unless the Contractor disclosed its intention to do so in the SOW Documents. On the Contractor's request, the State will incorporate into any copies of a custom Deliverable any proprietary notice that the Contractor included with the original copy, if that notice is reasonably necessary to protect the Contractor's interest in any Pre-existing Materials contained in the custom Deliverable.

Subject to the limitations and obligations of the State with respect to Pre-existing Materials, the State may make all custom Deliverables available to the general public without any proprietary notices of any kind.

For Deliverables that include custom materials such as software, scripts, or similar computer instructions developed for the State, the State is entitled to the source material. Scripts and similar functionality may not be locked or otherwise protected from access by the State, unless the State has any passwords or other tools necessary to access the material. Source material must include annotations or comments according to industry standards. Further, the State is entitled (upon its request) to a copy of any working papers, and design and architectural materials, such as schemas, that the Contractor has developed during the performance of the Project that would reasonably assist the State in using the Deliverables that include source materials or that would help the State protect its interests in the Deliverable or update, modify, or otherwise maintain the Deliverable.

The rights and license provided are subject to payment for the applicable Deliverable (or services giving rise thereto) by the State.

To the extent any Pre-existing Materials provided to the State hereunder constitutes inventory within the meaning of section 471 of the Internal Revenue Code, such Pre-existing Materials are licensed to the State by Contractor as agent for its product company subsidiary on the terms and conditions contained herein. The rights granted in this "Ownership of Deliverables" Section do not apply to any intellectual property (including any modifications or enhancements thereto or derivative works based thereon) that is subject to a separate license agreement between the State and Contractor or any third party (including,

Contractor's affiliates) and do not apply to Contractor's proprietary uFACTS for PUA/DUA tool, which is Pre-existing Material of Contractor and Contractor grants the State the license set forth in the second paragraph of this section, even if not incorporated into a Deliverable, except that the State may only use the uFACTS for PUA/DUA tool for its own business purposes for PUA/DUA and may not distribute it. The uFACTS for PUA/DUA shall not be deemed to be a Deliverable.

The Contractor may use Confidential Information only as necessary for Contractor's performance under or pursuant to rights granted in this Agreement and for no other purpose. The Contractor's limited right to use Confidential Information expires upon expiration or termination of this Agreement for any reason. The Contractor's obligations of confidentiality and non-disclosure survive termination or expiration for any reason of this Agreement.

License in Commercial Material.
This Section does not apply to this Agreement unless the parties mutually agree in writing via an amendment to this Agreement that this Section applies, in which case the parties will specifically identify the Commercial Material that is subject to this Section.

As used in this section, "Commercial Material" means anything, except the Contractor's proprietary uFACTS for PUA/DUA tool, that the Contractor or a third party has developed at private expense, is commercially available in the marketplace, subject to intellectual property rights, and readily copied through duplication on magnetic media, paper, or other media, in all cases that are specifically identified as "Commercial Material" in an amendment to this Agreement. Examples include written reports, books, pictures, videos, movies, computer programs, and computer source code and documentation.

Any Commercial Material that the Contractor intends to deliver as a Deliverable must have the scope of the license granted in such material disclosed in the SOW Documents or as an attachment referenced in the SOW Documents, if that scope of license is different from the scope of license contained in this section for Commercial Materials.

Except for Commercial Material that is software ("Commercial Software"), if the Commercial Material is copyrighted and published material, then the State will have the rights permitted under the federal copyright laws for each copy of the Commercial Material delivered to it by the Contractor.

Except for Commercial Software, if the Commercial Material is patented, then the State will have the rights permitted under the federal patent laws for each copy of the Commercial Material delivered to it by the Contractor.

Except for Commercial Software, if the Commercial Material consists of trade secrets, then the State will treat the material as confidential. In this regard, the State will assume all obligations with respect to the Commercial Material that the Contractor assumes under the Confidentiality section of this Contract with respect to the State's Confidential Information. Otherwise, the State will have the same rights and duties permitted under the federal copyright laws for each copy of the Commercial Material delivered to it by the Contractor, whether or not the material is copyrighted when delivered to the State.

For Commercial Software, the State will have the rights in items (1) through (6) of this section with respect to the software. The State will not use any Commercial Software except as provided in the six items below or as expressly stated otherwise in this Contract. The Commercial Software may be:

1. 1. Used or copied for use in or with the computer or computers for which it was acquired, including use at any State installation to which such computer or computers

may be transferred;

2. 2. Used or copied for use in or with a backup computer for disaster recovery and disaster recovery testing purposes or if any computer for which it was acquired is inoperative;
3. 3. Reproduced for safekeeping (archives) or backup purposes;
4. 4. Modified, adapted, or combined with other computer software, but the modified, combined, or adapted portions of the derivative software incorporating any of the Commercial Software will be subject to same restrictions set forth in this Contract;
5. 5. Disclosed to and reproduced for use on behalf of the State by support service contractors or their subcontractors, subject to the same restrictions set forth in this Contract; and
6. 6. Used or copied for use in or transferred to a replacement computer.

Commercial Software delivered under this Contract is licensed to the State without disclosure restrictions unless it is clearly marked as confidential or secret. The State will treat any Commercial Software that is marked as confidential or secret as Confidential Information to the extent that such is actually the case.]]

PART FOUR: REPRESENTATIONS, WARRANTIES, AND LIABILITIES

General Warranties. The Contractor warrants that the recommendations, guidance, and performance of the Contractor under this Contract will: (1) be in accordance with sound professional standards industry standards, and performs materially in accordance with the applicable user guide and the requirements of this Contract; and (2) unless otherwise provided in the SOW Documents, be the work solely of the Contractor or its subcontractors. The Contractor also warrants that no Deliverable will infringe on the intellectual property rights of any third party; and (2) the Contractor's work and the Deliverables resulting from that work will be merchantable and fit for the particular purposes described in the SOW Documents.

Additionally, with respect to the Contractor's activities under this Contract, the Contractor warrants that: (1) the Contractor has the right to enter into this Contract; (2) the Contractor has not entered into any other contracts or employment relationships that restrict the Contractor's ability to perform the contemplated services; (3) the Contractor will observe and abide by all applicable laws and regulations, including those of the State regarding conduct on any premises under the State's control and security for the State's data, systems, and networks; (4) the Contractor has the right and ability to grant the license granted in any Deliverable in which title does not pass to the State; and (5) the Contractor is not subject to any unresolved findings of the Auditor of State under Revised Code Section 9.24 and will not become subject to an unresolved finding that prevents the extension or renewal of this Contract.

The warranties regarding conformance with industry standards and the requirements of the Contract, material defects, merchantability, and fitness are one-year warranties or warranties limited to the term of this Contract, if less than one year. All other warranties will be continuing warranties. If any portion of the Work fails to comply with these warranties, and the Contractor is so notified in writing prior to the end of the applicable warranty period, the Contractor must timely correct such failure or must refund the amount of the compensation paid for such portion of the Work giving rise to such failure. The Contractor also must indemnify the State for any direct damages and claims by third parties based on a breach of the infringement warranty. This obligation of indemnification and to make warranty repairs will not apply where the State has modified or misused the Deliverable and the claim is based on the modification or misuse. The State will give the Contractor notice of any such claim as soon as reasonably practicable. If a successful claim of infringement is made, or if the Contractor reasonably believes that an infringement claim that is pending may actually succeed, the Contractor must do one of the following things: (1) modify the Deliverable so that it is no longer infringing; (2) replace the Deliverable with an equivalent or better item; (3) acquire the right for the State to use the infringing Deliverable as it was intended for the State to use under this Contract; or (4) remove the Deliverable and refund the amount the State paid for the Deliverable and the amount of any other Deliverable or item that requires the availability of the infringing Deliverable for it to be useful to the State.

The warranties set forth in this Section shall not apply with respect to software that is subject to a separate license agreement.

Software Warranty.
This "Software Warranty" Section does not apply to this Agreement unless the parties mutually agree in writing via an amendment to this Agreement that this Section applies, in which case the parties will identify in such amendment the specific software Deliverable to which this Section applies.

If this Contract involves software, as a Deliverable, then, on acceptance and for 12 months after the date of acceptance of any Deliverable that includes software, the Contractor warrants as to all software developed under this Contract that: (a) the software will operate on the computer(s) for which the software is intended in the manner described in the relevant software documentation, the Contractor's Proposal, and the SOW Documents; (b) the software will be free of any material defects; (c) the Contractor will deliver and maintain relevant and complete software documentation, commentary, and source code; and (d) the source code language used to code the software is readily available in the commercial market, widely used and accepted for the type of programming involved, and support programming in the language is

reasonably available in the open market; and (e) the software and all maintenance will be provided in a professional, timely, and efficient manner.

For Commercial Software licensed from a third party that is incorporated into a Deliverable, and for which the State has not approved a separate license agreement governing that Commercial Software's warranties as part of the SOW process, the Contractor represents and warrants that it has done one of the following things: (a) obtained the right from the third-party licensor to commit to the warranties and maintenance obligations in this Section; (b) obtained a binding commitment from the licensor to make those warranties and maintenance obligations directly to the State; or (c) fully disclosed in the SOW Documents any discrepancies between the requirements of this section and the commitment the third party licensor has made.

In addition, for Commercial Software that is incorporated into a Deliverable, the Contractor will: (a) maintain or cause the third-party licensor to maintain the Commercial Software so that it operates in the manner described in the SOW Documents (or any attachment referenced in the SOW Documents) and relevant Commercial Software documentation; (b) supply technical bulletins and updated user guides; (c) supply the State with updates, improvements, enhancements, and modifications to the Commercial Software and documentation and, if available, the commentary and the source code; (d) correct or replace the Commercial Software and/or remedy any material programming error that is attributable to the Contractor or the third-party licensee; (e) maintain or cause the third-party licensor to maintain the Commercial Software and documentation to reflect changes in the subject matter the Commercial Software deals with; (f) maintain or obtain a commitment from the third-party licensor to maintain the Commercial Software so that it will properly operate in conjunction with changes in the operating environment in which it is designed to operate.

For purposes of the warranties and the delivery requirements in this Contract, software documentation means well written, readily understood, clear, and concise instructions for the software's users as well as a system administrator. The software documentation will provide the users of the software with meaningful instructions on how to take full advantage of all of the capabilities designed for end users. It also means installation and system administration documentation for a system administrator to allow proper control, configuration, and management of the software. Source code means the uncompiled operating instructions for the software. However, the Contractor will not be obligated to provide source code for Commercial Software unless it is readily available from the licensor. The source code must be provided in the language in which it was written and will include commentary that will allow a competent programmer proficient in the source language to readily interpret the source code and understand the purpose of all routines and subroutines contained within the source code.

GENERAL EXCLUSION OF WARRANTIES. THE CONTRACTOR MAKES NO WARRANTIES, EXPRESS OR IMPLIED, OTHER THAN THOSE EXPRESS WARRANTIES CONTAINED IN THIS CONTRACT.

Indemnity for Property Damage and Bodily Injury. The Contractor must indemnify the State for all liability and expense resulting from bodily injury to any person (including injury resulting in death) and damage to tangible or real property arising out of Contractor's negligence or other tortious conduct in the performance of this Contract, provided that such bodily injury or property damage is due to the negligence or other tortious conduct of the Contractor, its employees, agents, or subcontractors. The Contractor will not be responsible for any damages or liability to the extent caused by the negligence or willful misconduct of the State, its employees, other contractors, or agents.

Limitation of Liability. Neither party will be liable for any indirect, incidental, or consequential loss or damage of the other party, including but not limited to lost profits, even if the parties have been advised, knew, or should have known of the possibility of such damages. Additionally, neither party will be liable to the other for direct or other damages arising from or relating to this Contract in excess of two times the Not-To-Exceed Fixed Price in this Contract. The limitations in this paragraph do not apply to: (i) any

obligation of the Contractor to indemnify the State against claims made against it pursuant to the indemnity for Property Damage and Bodily Injury; or (ii) other damages arising from bodily injury (including death) or personal injury or property damage caused by the Contractor's negligence or other tortious conduct.

PART FIVE: ACCEPTANCE AND MAINTENANCE

Passage of Title. Title to any Deliverable will pass to the State only on acceptance of the Deliverable as described in Attachment Two and in accordance with the Ownership of Deliverables above. All risk of loss, regardless of the cause, will remain with the Contractor until title to the Deliverable passes to the State.

Software Maintenance.
This "Software Maintenance" Section does not apply to this Agreement unless the parties mutually agree in writing via an amendment to this Agreement that this Section applies, in which case the parties will identify in such amendment the specific software Deliverable to which this Section applies.

If this Contract involves software as a Deliverable then, during the warranty period, as well as any optional maintenance periods that the State exercises, the Contractor must correct any material programming errors that are attributable to the Contractor within a reasonable period of time. However, the State must notify the Contractor, either orally or in writing, of a problem with the software and provide sufficient information for the Contractor to identify the problem.

The Contractor's response to a programming error will depend upon the severity of the problem. For programming errors that slow the processing of data by a small degree, render minor and non-mandatory functions of the System inoperable or unstable, or require users or administrators to employ workarounds to fully use the software, Contractor will respond to the request for resolution within four business hours. Furthermore, the Contractor must begin working on a proper solution for the problem within one business day, dedicating the resources required to fix the problem. For any defects with more significant consequences, including those that render key functions of the system inoperable or significantly slow processing of data, the Contractor will have support personnel respond within two business hours of notice. The Contractor also must begin working on a proper solution for the problem immediately after responding and, if requested, provide on-site assistance and dedicate all available resources to resolving the problem.

For software classified as Commercial Software in the Ownership of Deliverables section and for which the State has not signed a separate license agreement, the Contractor must acquire for the State the right to maintenance for one year. That maintenance must be the third-party licensor's standard maintenance program, but at a minimum, that maintenance program must include all, updates, patches, and fixes to the software. It also must include a commitment to keep the software current with the operating environment in which it is designed to function (and, if applicable, the subject matter covered by the software) and to correct material defects in the software in a timely fashion. Additionally, the Contractor must obtain a commitment from the licensor to make maintenance available for the product for at least four years after the first year of maintenance. The Contractor also must obtain a commitment from the licensor to limit increases in the annual Fee for maintenance to no more than 7% annually. If the licensor is unable to provide maintenance during that five-year period, then the licensor must be committed to doing one of the following two things: (a) give the State a *pro rata* refund of the license fee based on a five-year useful life; or (b) release the source code for the software (except third party software) to the State for use by the State solely for the purpose of maintaining the copy(ies) of the software for which the State has a proper license. For purposes of receiving the source code, the State agrees to treat it as confidential and to be obligated to the requirements under the Confidentiality section of this Contract with respect to the source code. That is, with respect to the source code that the State gets under this section, the State will do all the things that the Confidentiality section requires the Contractor to do in handling the State's Confidential Information.

PART SIX: CONSTRUCTION

Entire Document. This Contract is the entire agreement between the parties with respect to its subject matter and supersedes any previous agreements, whether oral or written.

The State and Contractor have separately executed a separate agreement for Contractor's proprietary uFACTS for PUA/DUA cloud hosted application (the "Cloud Services Agreement" or "CSA"), and the parties agree that the terms and conditions of the CSA shall exclusively govern the State's purchase and use of the such application. In addition, the State and Contractor agree to the uFACTS SOW General Terms and Conditions applicable to the performance of services described in the SOW Documents. As such, the parties further agree that any requirements for such application included in the SOW Documents are applicable to this Contract and Contractor's performance of services together with the performance of the solution as a whole, must meet the requirements as outlined in the SOW Documents.

Binding Effect. This Contract will be binding upon and inure to the benefit of the respective successors and assigns of the State and the Contractor.

Amendments – Waiver. No change to any provision of this Contract will be effective unless it is in writing and signed by both parties. The failure of either party at any time to demand strict performance by the other party of any of the terms of this Contract will not be a waiver of those terms. Waivers must be in writing to be effective, and either party may at any later time demand strict performance.

Severability. If any provision of this Contract is held by a court of competent jurisdiction to be contrary to law, the remaining provisions of this Contract will remain in full force and effect to the extent that such does not create an absurdity.

Construction. This Contract will be construed in accordance with the plain meaning of its language and neither for nor against the drafting party.

Headings. The headings used herein are for the sole sake of convenience and may not be used to interpret any section.

Notices. For any notice under this Contract to be effective, it must be made in writing and sent to the address of the appropriate contact provided elsewhere in the Contract, unless such party has notified the other party, in accordance with the provisions of this section, of a new mailing address. This notice requirement will not apply to any notices that this Contract expressly authorized to be made orally.

Continuing Obligations. The terms of this Contract will survive the termination or expiration of the time for completion of Project and the time for meeting any final payment of compensation, except where such creates an absurdity.

Time. Unless otherwise expressly provided, any reference in this document to a number of days for an action or event to occur means calendar days, and any reference to a time of the day, such as 5:00 p.m., is a reference to the local time in Columbus, Ohio.

Time is of the Essence. Contractor hereby acknowledges that time is of the essence for deliveries and performance of key milestones identified as such under this Contract, unless otherwise agreed to in writing by the parties, provided that Contractor is not responsible for delays caused by events, acts or omissions outside its control.

PART SEVEN: LAW AND COURTS

Compliance with Law. The Contractor must comply with all applicable federal, state, and local laws while performing under this Contract.

Drug-Free Workplace. The Contractor must comply with all applicable state and federal laws regarding keeping a drug-free workplace. The Contractor must make a good faith effort to ensure that all the Contractor's Personnel, while working on state property, will not have or be under the influence of illegal drugs or alcohol or abuse prescription drugs in any way.

Conflicts of Interest and Ethics Compliance Certification. None of the Contractor's Personnel may voluntarily acquire any personal interest that conflicts with their responsibilities under this Contract. Additionally, the Contractor may not knowingly permit any public official or public employee who has any responsibilities related to this Contract or the Project to acquire an interest in anything or any entity under the Contractor's control, if such an interest would conflict with that official's or employee's duties. The Contractor must disclose to the State knowledge of any such person who acquires an incompatible or conflicting personal interest related to this Contract. The Contractor also must take steps to ensure that such a person does not participate in any action affecting the work under this Contract. However, this will not apply when the State has determined, in light of the personal interest disclosed, that person's participation in any such action would not be contrary to the public interest.

Ohio Ethics Law and Limits on Political Contributions. The Contractor certifies that it is currently in compliance and will continue to adhere to the requirements of the Ohio ethics laws. The Contractor also certifies that all applicable parties listed in Ohio Revised Code Section 3517.13 are in full compliance with Ohio Revised Code Section 3517.13.

Unresolved Finding for Recovery. If the Contractor was subject to an unresolved finding of the Auditor of State under Revised Code Section 9.24 on the date the parties sign this Contract, the Contract is void. Further, if the Contractor is subject to an unresolved finding of the Auditor of State under Revised Code Section 9.24 on any date on which the parties renew or extend this Contract, the renewal or extension will be void.

Equal Employment Opportunity. The Contractor will comply with all state and federal laws regarding equal employment opportunity and fair labor and employment practices, including Ohio Revised Code Section 125.111 and all related Executive Orders.

Before a contract can be awarded or renewed, an Affirmative Action Program Verification Form must be submitted to the Department of Administrative Services Equal Opportunity Division to comply with the affirmative action requirements. Affirmative Action Verification Forms and approved Affirmative Action Plans can be found by going to the Ohio Business Gateway at: http://business.ohio.gov/efiling/

Use of MBE and EDGE Suppliers. The State encourages Contractor to purchase goods and services from Minority Business Enterprises (MBE) and Encouraging Diversity, Growth, and Equity (EDGE) suppliers.

Security & Safety Rules. When using or possessing State data or accessing State networks and systems, the Contractor must comply with all applicable State rules, policies, and regulations regarding data security and integrity. And when on any property owned or controlled by the State, the Contractor must comply with all security and safety rules, regulations, and policies applicable to people on those premises.

Prohibition of the Expenditure of Public Funds for Offshore Services. No State Cabinet, Agency, Board or Commission will enter into any contract to purchase services provided outside the United States or that allows State data to be sent, taken, accessed, tested, maintained, backed-up, stored, or made

available remotely outside (located) of the United States. Notwithstanding any other terms of this Contract, the State reserves the right to recover any funds paid for services the Contractor performs outside of the United States for which it did not receive a waiver. The State does not waive any other rights and remedies provided the State in the Contract.

The Contractor must complete the Contractor/Subcontractor Affirmation and Disclosure form affirming the Contractor understands and will meet the requirements of the above prohibition. During the performance of this Contract, the Contractor must not change the location(s) disclosed on the Affirmation and Disclosure Form, unless a duly signed waiver from the State has been attained to perform the services outside the United States.

Injunctive Relief. Nothing in this Contract is intended to limit the State's right to injunctive relief, if such is necessary to protect its interests or to keep it whole.

Assignment. The Contractor may not assign this Contract or any of its rights or obligations under this Contract without the prior, written consent of the State. The State is not obligated to provide its consent to any proposed assignment.

Governing Law. This Contract will be governed by the laws of Ohio, and venue for any disputes will lie exclusively with the appropriate court in Franklin County, Ohio.

Registration with the Secretary of State. By providing a Charter Number and signature within the Certification Offer Letter, the Contractor attests that the Contractor is:

An Ohio corporation that is properly registered with the Ohio Secretary of State; or

A foreign corporation, not incorporated under the laws of the state of Ohio, but is registered with the Ohio Secretary of State pursuant to Ohio Revised Code Sections 1703.01 to 1703.31, as applicable.

Any foreign corporation required to be licensed under O.R.C. § 1703.01-1703.31, which transacts business in the state of Ohio, without being so licensed, or when its license has expired or been canceled, shall forfeit not less than $250.00 nor more than ten thousand dollars. No officer of a foreign corporation http://codes.ohio.gov/orc/1703.01 shall transact business in the state of Ohio, if such corporation is required by O.R.C. § 1703.01-1703.31 to procure and maintain a license, but has not done so. Whoever violates this is guilty of a misdemeanor of the fourth degree. Questions regarding registration should be directed to (614) 466-3910, or visit http://www.sos.state.oh.us.

Boycotting

Pursuant to Ohio Revised Code 9.76 (B) Contractor warrants that Contractor is not boycotting any jurisdiction with whom the State of Ohio can enjoy open trade, including Israel, and will not do so during the contract period.

PART EIGHT: GENERAL REQUIREMENTS FOR CLOUD SERVICES

This Part Eight does not apply to this Agreement unless the parties mutually agree in writing via an amendment to this Agreement that this Section applies, in which case the parties will identify in such amendment the specific Service subscriptions to which this Section applies.
.

Standards
All Service subscriptions must provide a Service that maintains a redundant infrastructure that will ensure access for all of the State's enrolled users in case of a failure at any one of the Contractor locations, with effective contingency planning (including back-up and disaster recovery capabilities) and 24x7 trouble shooting service for inquiries, outages, issue resolutions, etc. All such Services must be dependable and provide response rates that are as good as or better than industry standards. They also must meet the

Service Level Agreements (“SLAs”) provided in the SOW and be supported with sufficient connectivity and computing resources to handle reasonably anticipated peak demand, and the Contractor must ensure that sufficient bandwidth and computing resources are dedicated to the Services to meet peak demand times without material degradation in performance.

User access to the Services must be capable of being integrated with the State’s Active Directory or other Lightweight Directory Access Protocol (LDAP) service to support single sign-on capability for users and to ensure that every user is tied to an Active Directory or other LDAP account and to prevent user access when a user is disabled or deleted in the State’s Active Directory or other LDAP service.

At no cost to the State, the Contractor must immediately remedy any issues, material weaknesses, or other items identified in each audit as they pertain to the Services.

The above standards are in addition to those contained in the State Architecture Security Privacy and Data Handling Supplement.

Object Reassignment

Any Service subscriptions that are provided by the number of items that may be used by or in conjunction with it, such as nodes, users, or connections (“Objects”), may be reassigned to other, similar Objects within the State at any time and without any additional fee or charge. For example, a named user subscription may be assigned to another user. But any such reassignment must be in conjunction with termination of use by or with the previous Object, if such termination is required to keep the total number of licensed Objects within the scope of the applicable subscription. Should the State require a special code, a unique key, or similar item to reassign the subscription as contemplated by this section, the Contractor will provide such a code, key, or similar item to the State at any time and without a fee or charge.

Generated Files

“Generated Files” are files storing information, instructions, or data that the State creates or modifies using the Contractor’s Services and in which the data or other information was provided or created by the State. Examples of such files could include, among others, text files generated with a word processor, data tables created with a database engine, and image files created with a graphics application. Applications consisting of instruction sets created with a programming language that the Contractor provided to the State also would be considered Generated Files. As between the State and the Contractor, the State will own all Generated Files that the State prepares by using the Services, excluding such portions of the Generated Files that consist of embedded portions of the Software. The Contractor or its licensors will retain ownership of any portions of the Software embedded into Generated Files. But the Contractor grants to the State a nonexclusive, royalty-free right to reproduce and distribute to third parties any portions of the intellectual property embedded in any Generated Files that the State creates while using the Services in the manner in which the Services are designed to be used. In the State’s distribution of the Generated Files, the State may not use the Contractor’s name, logo, or trademarks, except to the extent that such are incorporated in such Generated Files by the design of a Service when used as intended.

Additional Contractor Warranties

In addition to the other warranties contained in this Contract, the Contractor warrants the following:

i. The Services will perform materially in accordance with the applicable user guide and the requirements of this Agreement.
ii. The functionality of the Services will not be materially decreased during a subscription term.
iii. It will not transmit viruses, worms, time bombs, Trojan horses or other harmful or malicious code, files, scripts, agents or programs (“Malicious Code”) to the State.

Third-Party Suppliers

The Contractor must incorporate the costs of any third-party supplies and services in the Contractor’s fees identified in the Contract.

The Contractor’s use of other suppliers does not mean that the State will pay for them. The Contractor will be solely responsible for payment of its suppliers and any claims of those suppliers for any failure of the Contractor to meet its obligations under this Contract in the required manner. The Contractor will hold the State harmless and indemnify the State against any such claims.

The Contractor assumes responsibility for all Cloud Services provided under this Contract whether it or one of its suppliers provides them in whole or in part. Further, the Contractor will be the sole point of contact

with regard to contractual matters, including payment of all charges resulting from the Contract and all service and support requests.

Upgrades

The State has the option anytime during the Agreement's term to upgrade to a new technology or Service offering with the Contractor without incurring any charges for terminating the existing technology or Service offering before the agreed upon term of the Order.

Acceptance

The acceptance procedure for setup or installation of any Cloud Services will be a review by the State to ensure that it meets the performance standards and other requirements in the Contract and that the setup or installation has been done in a professional manner and that the Cloud Services itself meets all requirements. For other Cloud Services not requiring setup or installation, the acceptance procedure will be a review by the State to ensure the Cloud Services comply with the performance requirements in the Contract. In addition to the requirements of the Contract, if ordering documents such as a statement of work are authorized in the Contract, the review will include any additional requirements in the applicable order form. The State will have up to 15 days after the setup, installation, or establishment of the Cloud Services to do this. The State will issue a formal letter of acceptance if setup, installation, or other Service meets the requirements in the Contract. If the setup, installation, or other Service does not meet the requirements of the Contract, the State will issue a written notice of noncompliance.

If the State issues a noncompliance letter, the Contractor will have 30 days to correct the problems listed in the letter. If the State has issued a noncompliance letter, the Cloud Services, installation, or set up will not be accepted until that State issues a letter of acceptance indicating that each problem noted in the noncompliance letter has been cured. If the problems have been fixed during the 30-day period, the State will issue the acceptance letter within 15 days after all defects have been fixed. If the Contractor fails to correct the defect(s), the applicable Order(s) will terminate without cost or obligation to the State, and the State will be entitled to a full refund of any payments made for the Service, setup, and installation.

The applicable Contract may provide additional or alternative acceptance procedures, but no Order may change the acceptance processes.

State Reporting Requirements

The Contractor must provide the State with a recap of all Cloud Services provided to the State on a monthly basis. Additional, specific reporting data requirements may be outlined in the Contract(s).

Termination Service

The Contractor will provide to the State termination services ("Termination Service") according to the terms of the Disentanglement Plan, in connection with the termination or expiration without renewal of this Contract.

Termination Service means, to the extent requested by a State, the provisioning of such assistance, cooperation, and information as is reasonably necessary to enable a smooth transition of the Services to the State or its designated third- party provider ("Successor") in accordance with the Disentanglement Plan. As part of Termination Service, the Contractor will, in accordance with the Disentanglement Plan, manage the migration, to the extent requested and provide such information as the State may reasonably request relating to the number and function of each of the Contractor personnel performing the Services, and Contractor will make such information available to the Successor designated by the State.

Disentanglement Plan

Upon the State's request, the Contractor will prepare a disentanglement plan with the input from the State and the Successor, if there is one.

The contents of the Disentanglement Plan will be as mutually agreed upon and will include at least the following activities, unless the State and the Contractor agree otherwise:

- Documentation of existing and planned support activities.
- Identification of the Service and related positions or functions that require transition and a schedule, plan, and procedures for the State or the Successor assuming or reassuming responsibility.
- Description of actions to be taken by the Contractor, State, and, if applicable, the Successor in performing the disentanglement.
- Description of how the transfer of (i) relevant information regarding the Services, (ii) resources (if any), and (iii) operations will be achieved.

- Description in detail of any dependencies the State and, if applicable, the Successor must fulfill for the Contractor to perform the Termination Service (including an estimate of the specific staffing and time required).
- Inventory of documentation and work products required to facilitate the transition of responsibilities.
- Identification of significant potential risk factors relating to the transition and in designing plans and contingencies to help mitigate the risk.
- A timeline for the transfer of each component of the Termination Service (including key milestones to track the progress of the transfer).
- A schedule and plan for Contractor's return to the State of (i) the systems held by the Contractor and belonging to the State, and (ii) all documents, records, files, tapes, and disks in Contractor's possession that belong to the State or relate to the migrating system(s).

Disentanglement Management Team
The Contractor will provide a project manager who will be responsible for Contractor's overall performance of the Termination Service and who will be the primary point of contact for the State and any Successor during the transfer. The State also will appoint a project manager who will be the primary point of contact for Contractor during the disentanglement period.
Operational Transfer
The Contractor also will provide the State and any Successor access to those resources described in the Disentanglement Plan reasonably necessary during the planning and execution of the Termination Service.

Support
Service Support Generally
During the term of any Order, the Contractor will provide the State with telephonic assistance and advice for using all Cloud Services covered by the Order. The Contractor also will provide troubleshooting and problem resolution, including on site whenever necessary. The manner in which the Contractor provides support will be governed by the Contractor's written policies and programs described in the applicable documentation or other materials that the Contractor uses to notify its customers generally of such policies. But regardless of the Contractor's policies and programs, unless otherwise agreed in the applicable Contract, in all cases such support must comply with the requirements of this Contract and the applicable Contract(s). And the Contractor must provide the support in a competent, professional, and timely manner.
Equipment Support Generally
For any equipment used to provide the Cloud Services, remedial equipment maintenance by the Contractor will be completed within eight hours after notification by the State that maintenance is required. In the case of preventative maintenance, the Contractor will perform such in accordance with the manufacturer's published schedule and specifications. If maintenance is not completed within eight hours after notification by the State, the Contractor will be in default. Failure of the Contractor to meet or maintain these requirements will provide the State with the same rights and remedies as specified elsewhere in this Contract for default, except that the Contractor will only have eight hours to remedy a default. Nothing contained herein will limit the application of any credits for failure to meet any SLAs in the Contract. The Contractor will provide adequate staff to provide the maintenance required by this Contract.
Support Parameters
The State may initiate support requests for problems it encounters with the Cloud Services by telephone, email, Internet, or fax, and the Contractor must maintain lines of communication that support all four forms of communication.
The Contractor must make support available during the hours of operations, as defined in Supplement one (the "Support Window"), and it must do so by staffing its support function with an adequate number of qualified personnel to handle its traditional volume of calls. The State's technical staff may contact any support center that the Contractor maintains, and they may choose to do so based on convenience, proximity, service hours, languages spoken, or otherwise.
Incident Classification
The Contractor must classify and respond to support calls by the underlying problem's effect on a State. In this regard, the Contractor may classify the underlying problem as critical, urgent, or routine. The guidelines

for determining the severity of a problem and the appropriate classification of and response to it are described below.

The Contractor must designate a problem as “critical” if the Service is functionally inoperable, the problem prevents the Service or a major component or function from being used.

The Contractor must classify a problem as “urgent” if the underlying problem significantly degrades the performance of the Service or a major function or component of it or materially restricts a State’s use of the Service. Classification of a problem as urgent rather than critical assumes that the State still can conduct business with the Service and response times are consistent with the needs of the State for that type of Service.

Finally, the Contractor may classify a support call as “routine” if the underlying problem is a question on end use or configuration of the Service. It also may be classified as routine when the problem does not materially restrict the State’s use of the Service.

The Contractor must apply the above classifications in good faith to each call for support, and the Contractor must give due consideration to any request by the State to reclassify a problem, taking into account the State’s unique business and technical environments and any special needs it may have.

Incident Response

The Contractor must respond to critical problems by ensuring that appropriate managerial personnel are made aware of the problem and that they actively track and expedite a resolution.

The Contractor must assign support personnel at the appropriate level to the problem, and those personnel must arrive at the State’s site or other location from where the problem has arisen, if appropriate for proper resolution. At the request of the State, the Contractor’s personnel must maintain hourly contact with the State’s technical staff to keep the State abreast of efforts being made to solve the problem. The Contractor also must provide the State’s technical staff with direct access to the Contractor’s support personnel, if appropriate, who are assigned to the problem.

The Contractor must respond to urgent problems by assigning support personnel at the appropriate level to the problem, and those personnel must arrive at the State’s site or other location from where the problem has arisen, if appropriate for proper resolution. At the request of the State, the Contractor’s personnel must maintain hourly contact with the State’s technical staff to keep the State abreast of efforts being made to solve the problem. The Contractor also must provide the State’s technical staff with direct access to the Contractor’s support personnel, if appropriate, who are assigned to the problem.

The Contractor must respond to routine problems by assigning support personnel at the appropriate level to the problem. For routine calls that involve end usage and configuration issues rather than bugs or other technical problems, the Contractor’s first or second level support personnel must provide the State’s technical staff with telephonic assistance on a non-priority basis.

The Contractor must comply with the FCC's Telecommunications Service Priority Program in setting Service installation and restoration priorities for all Cloud Services the State has registered for such preferential treatment under that program.

Response Times

The maximum time that the Contractor takes to respond initially to a support request may vary based upon the classification of the request. During the Support Window, the Contractor’s response time for a critical support request will be less than one hour. The Contractor’s response time for an urgent request must be less than four hours during the Support Window. And the Contractor’s response time for a routine support request must be less than one day during the Support Window. The applicable Contract may provide for shorter response times for a particular Service, and nothing contained herein will limit the application of any credits for failure to meet any SLAs in the applicable Contract.

Escalation Process

Any support call that is not resolved must be escalated to the Contractor’s management under the following parameters. Unresolved problems that are classified as critical must be escalated to the Contractor’s support manager within one hour and to the director level after four hours. If a critical problem is not resolved within one day, it must escalate to the CEO level after two days. The Contractor’s support staff will escalate unresolved urgent problems to its support manager within three hours, to the director level after one day, and to the CEO level after two days.

State Obligations

To facilitate the Contractor meeting its support obligations, the State must provide the Contractor with the information reasonably necessary to determine the proper classification of the underlying problem. They

also, must assist the Contractor as reasonably necessary for the Contractor's support personnel to isolate and diagnose the source of the problem. Additionally, to assist the Contractor's tracking of support calls and the resolution of support issues, the State must make a reasonable effort to use any ticket or incident number that the Contractor assigns to a particular incident in each communication with the Contractor.

Relationship to SLAs

The Contractor's support obligations are in addition to the SLAs in the Contract. Furthermore, the SLAs may provide for credits to the State even though the Contractor is meeting its support obligations hereunder.

Service Level Guarantee and Credits

The Contractor will issue a credit allowance to the State affected by a Service outage, as defined in the Service Level Contract contained in the applicable Contract. The credit will appear on the State's next invoice, or if the State so requests, the Contractor will issue a check to the State as payment within 30 days of the request.

Deloitte Consulting LLP
uFACTS PUA/DUA Cloud Services Agreement (CSA)
April 13, 2020

THIS CLOUD SERVICES CONTRACT ("Agreement") is by and between Deloitte Consulting LLP ("Contractor"), having an office at 180 East Broad Street Suite 1400, Columbus, OH 43215, and the State of Ohio ("State"), through its Department of Job and Family Services ("ODJFS"), having its principal place of business at 30 East Broad Street, 32nd Floor, Columbus, OH 43215. The State and the Contractor also are sometimes referred to jointly as the "Parties" or individually as a "Party". The effective date of this Agreement is the date it is signed on behalf of the State ("Effective Date").

1. General Information

1.1. Organization

This Agreement covers a license to Contractor's proprietary uFACTS for Pandemic Unemployment Assistance and Disaster Unemployment Assistance (PUA/DUA) cloud hosted application through the Service Attachment attached hereto ("Service Attachment") that describes the uFACTS for PUA/DUA cloud offering ("Service") that the Contractor makes available to its customers by license and that it is authorized to license to the State. The Service Attachment describes the Services the Contractor offers under this Agreement, along with any special terms or conditions applicable only to those Services, descriptions of those Services, features, and all fees associated with such Services, as well as any other provisions to which the Parties have agreed with respect to those Services. Such Service Attachment is incorporated into this Agreement and is a part hereof.

1.2. Subscribers

A "Subscriber" means State entities such as agencies, boards, and commissions (sometimes referred to as "State Entities") that place orders ("Orders") hereunder for any of the Services identified hereunder by execution with Contractor of a Service Attachment incorporated into this Agreement. For purposes of this Agreement, an Order is synonymous with the Service Attachment described herein.

1.3. Term

The current General Assembly cannot commit a future General Assembly to any expenditure. Therefore, this Agreement along with the Service Attachment will automatically expire at the end of the State's current biennium, which is June 30, 2021.

1.4. Agreement – Renewal

The State and Contractor may renew this Agreement in the next biennium by written agreement of the decision to do so. Renewal requests will be initiated by the State in writing at least 30 days before the expiration of the then current term. This expiration and renewal procedure will also apply to the end of any subsequent biennium.

1.5. Service Attachment(s) – Renewal

As part of the renewal of this Agreement, the Service Attachment will also renew for the next fiscal year by mutual written agreement of the Contractor and State of the decision to do so subject to any license end date set forth in the Service Attachment. Renewal requests will be initiated by the State at least 30 days before the expiration of the then current term. This expiration and renewal procedure will also apply to any subsequent fiscal year.

For each renewal, the Parties will agree in writing to the pricing of Services under the Service Attachment for such renewal.

1.6. Relationship of the Parties and Subscribers

The Contractor is an independent contractor and is not an agent, servant, or employee of the State. The Contractor is engaged as an independent business and has complied with all applicable federal, state, and local laws regarding business permits and licenses of any kind, including but not limited to any insurance coverage, workers' compensation, or unemployment compensation that is required in the normal course of business and will assume all responsibility for any federal, state, municipal, or other tax liabilities. Additionally, as an independent contractor, the Contractor is not a public employee and is not entitled to contributions from the State to any public employee retirement system or any other benefit of public employment.

Further, any individual providing personal services under this Agreement is not a public employee for purposes of Chapter 145 of the Ohio Revised Code. And unless the Contractor is a "business entity" as that term is defined in ORC 145.037 ("an entity with five or more employees that is a corporation, association, firm, limited liability company, partnership, sole proprietorship, or other entity engaged in business") the Contractor must have any individual performing work under this Agreement complete and submit to the ordering agency the Independent Contractor/Worker Acknowledgement form found at the following link:

https://www.opers.org/forms-archive/PEDACKN.pdf#zoom=80

The Contractor's failure to complete and submit the Independent/Worker Acknowledgement form before providing any Service or otherwise doing any work hereunder will serve as the Contractor's certification that the Contractor is a "Business entity" as the term is defined in ORC Section 145.037.

1.7. Audits and Reports

During the term of this Agreement and for three years after its termination, on reasonable notice and during customary business hours, the State may audit the Contractor's billing records that relate to the charges for the Services under this Agreement as necessary to confirm the accuracy of any billings or invoices under the Agreement. This audit right also will apply to the State's duly authorized representatives and any organization providing funding for any Order hereunder.

The Contractor must make such records and materials available to the State within 15 days after receiving the State's written notice of its intent to audit the Contractor's records and must notify the State as soon as the records are ready for audit.

If any audit reveals any material misrepresentation, overcharge to the State, or violation of the terms of this Agreement, the State will be entitled to recover its damages, including the cost of the audit.

The State will be entitled to any other reports that the Contractor makes generally available to its other customers without additional charge. The State's rights under this section will apply to all Services provided to all Subscribers under this Agreement, but a Subscriber's rights to reports will apply solely to Services it orders or receives under this Agreement.

1.8. Third-Party Suppliers

The Contractor must incorporate the costs of any third-party supplies and services in the Contractor's fees identified on the applicable Service Attachment under this Agreement.

The Contractor's use of other suppliers does not mean that the State will pay for them. The Contractor will be solely responsible for payment of its suppliers and any claims of those suppliers for any failure of the Contractor to make such payment. The Contractor will hold the State harmless and indemnify the State against any such claims.

The Contractor assumes responsibility for all Services provided under this Agreement whether it or one of its suppliers provides them in whole or in part. Further, the Contractor will be the sole point of contact for all contractual matters, including payment of all charges resulting from the Agreement and all Service requests.

1.9. Non-Exclusivity

This Agreement is non-exclusive and is not a requirements contract. Nothing herein prevents either Party from entering into similar agreements with other entities.

1.10. Conflict Resolution

If one Party believes the other Party has violated or is not complying with the terms of this Agreement or if any other dispute arises under this Agreement, the Party raising the matter may provide to the other Party written notice referencing this section and specifying the nature of the dispute (the "Dispute Notification"). The Parties then will seek to resolve the dispute in accordance with the procedures in this Section.

All disputes will be submitted first to the authorized State Representative (or designee) and the Contractor's Engagement Leader (or equivalent) for resolution. For 15 days from receipt of the Dispute Notification ("Dispute Date"), the authorized State Representative and Contractor's Account Manager will meet in person or by telephone as often as is reasonably necessary to discuss and attempt to resolve the dispute in good faith.

If after the 15 days identified above, the authorized State Representative and the Contractor's Account Manager are unable to resolve the dispute, the Parties will then submit the dispute to the State's IT Contract Manager (or designee) and to the Contractor's uFACTS for PUA/DUA leader (or equivalent) for resolution. For the next 15 days, the

State's IT Contract Manager and Contractor's Sales Director will meet in person or by telephone as often as is reasonably necessary to discuss and attempt to resolve the dispute in good faith.

If following the 15 days in the previous section, the State's IT Contract Manager and the Contractor's Sales Director are unable to resolve the dispute, the Parties will then submit the dispute to the State's Chief Information Officer ("CIO") or a designee and to the Contractor's Lead Client Service Principal (or equivalent executive) for resolution. For the next 15 days, the State's CIO and Contractor's Vice President will meet in person or by telephone as often as is reasonably necessary to discuss and attempt to resolve the dispute in good faith. If the State's CIO and Contractor's Vice President are unable to resolve the dispute within that time, the Parties will nevertheless continue to retain their rights to initiate formal proceedings hereunder.

The specific format for such discussions will be left to the discretion of the representatives of the State and Contractor responsible for attempting to resolve the dispute, but each Party will involve the business, technical, and legal resources reasonably necessary to attempt in good faith to resolve the dispute at the earliest possible time and without undue delay.

If the Parties are unable to resolve the dispute and the dispute involves a claim that the Contractor has overcharged for a Service, the State or affected Subscribers may withhold payment for any Services that are the subject of the dispute until the Parties arrive at an agreement to resolve the dispute, or a Party obtains a resolution in a court of competent jurisdiction.

Nothing in this section is intended to limit the rights provided under termination section of this Agreement or be a prerequisite to exercising those rights.

Once the dispute has been resolved, any payments withheld will be handled in the following manner:

> If the resolution was in favor of the State or one or more Subscribers, the Contractor will issue a credit on the next invoice for the affected Subscribers. If the credit exceeds the Service charges on the next invoice or an invoice will not be issued within 60 days of the resolution, the Contractor will issue payment in the form of a check in the amount exceeding the Service charges or for the full amount if an invoice will not be issued within 60 days. Any such checks must be issued within that 60-day period.
>
> If in favor of the Contractor, the affected Subscribers will submit appropriate payment within 30 days of receiving notification of the resolution at the office designated to receive the invoice.

In either of the above cases, the amount or amounts withheld by the State or Subscriber(s) will be taken into account in calculating any amount(s) due.

2. General Requirements for Cloud Services

2.1. Standards

All Service subscriptions must provide a Service that maintains a redundant infrastructure that will ensure access for all the State's authorized users in case of a failure at any one of the Contractor locations, with effective contingency planning (including back-up and disaster recovery capabilities) and maintenance and support as set forth in the Service Attachment to address trouble shooting service for inquiries, outages, issue resolutions, etc. All such Services must meet the Service Level Agreements ("SLAs") provided in the applicable Service Attachment and be supported with sufficient connectivity and computing resources to meet peak demand times without material degradation in performance.

Contractor will use commercially reasonable efforts to establish, maintain and comply with administrative, technical and physical safeguards on its infrastructure support services system that are designed to (a) protect the confidentiality, availability and integrity of the User data; (b) guard against security incidents; and (c) utilize equivalent safeguards in accordance with NIST Cyber Security Framework and NIST 800-53 Security Controls for a moderate baseline information system. In connection therewith, Contractor agrees to maintain and implement information security policies and procedures that address, at a minimum the following domains: information security policy, organization of information security, risk management, asset management, human resource security, physical and environmental security, electronic and wireless communications, access control, information systems acquisition, development and maintenance, information security incident management, business continuity management, encryption, vendor management, regulatory compliance. The contractor, in accordance with the Security Supplement, will develop a System Security Plan, that will be reviewed and accepted by the Agency.

Configuration Baselines of devices and applications within the solution must meet CIS Benchmarks established for that specific device or application type. The Contractor must maintain a robust boundary security capacity that incorporates generally recognized system hardening techniques. This includes determining which ports and services are required to support access to systems limiting access to only these points and disabling all others. To do this, the Contractor must use assets and techniques such as properly configured firewalls, a demilitarized zone for handling public traffic, host-to-host management, Internet protocol specification for source and destination, strong authentication, encryption, packet filtering, activity logging, and implementation of system security fixes and patches as they become available and employing appropriate intrusion and attack prevention and detection capabilities. Those capabilities must track unauthorized access and attempts to as well as attacks on the Contractor's infrastructure. Further, the Contractor must monitor and appropriately address information from its system tools used to prevent and detect unauthorized access to and attacks on the infrastructure. The Contractor must have a business continuity plan in place. The Contractor must integrate and provide export of the Logs into the State's Log Event Management (LEM) and Security Incident Management Systems (SIEM). The Contractor must test and update the IT disaster recovery portion of its business continuity plan at least annually. The plan must address procedures for response to emergencies and other business interruptions. Part of the plan must address backups at a location sufficiently remote from the facilities in case of unavailability at the primary site. The plan also must

address the rapid restoration, relocation, or replacement of resources associated with Service in the case of a disaster or other business interruption. The Contractor's business continuity plan must address short- and long-term restoration, relocation, or replacement of resources that will ensure the smooth continuation of operations related to Service.

The Service runs on Amazon Web Services (AWS) Commercial Cloud and the security standards and related practices set out for AWS on its website shall apply to the security responsibilities for AWS on its infrastructure. Agency data and application must be isolated and separated from any other customer data or application and not installed on any shared instance/resources. Agency Data are required to be hosted/stored within the Continental United States and is restricted from being hosted, stored, or accessed at or by any offshore location or entity respectively. Contractor will perform configuration review of operating system, application, and database settings. Contractor will also ensure software development personnel receive training in writing secure code. The solution must be capable of consuming Security Access Markup Language (SAML) 2.0 identity assertions or OpenID Connect (OAUTH), for SSO (Single Sign-On).

If the Service is cloud based, at the State's request beginning after June 2020, the Contractor must obtain an annual Service Organization Control 2 Type 2 (SOC 2 Type 2) report for the cloud hosting infrastructure managed by Contractor or FedRAMP Moderate Authorization. The audit will be at the sole expense of the Contractor and the results must be provided to the State upon written request within 30 days of its completion each year. State shall not disclose such SOC 2 Type 2/FedRAMP Report, or refer to such items in any communication, to any person or entity other than the State.

2.2. Object Reassignment

Any Service subscriptions that are provided by the number of items that may be used by or in conjunction with it, such as nodes, users, or connections ("Objects"), may be reassigned to other, similar Objects within the Subscriber's organization at any time and without any additional fee or charge subject to the pricing parameters for such Objects set forth in the Service Attachment. For example, a named user subscription may be assigned to another user. But any such reassignment must be in conjunction with termination of use by or with the previous Object, if such termination is required to keep the total number of licensed Objects within the scope of the applicable subscription. However, a reassignment cannot take place for purposes of avoiding purchasing an increased number of Objects as set forth in the Service Attachment. Should a Subscriber require a special code, a unique key, or similar item to reassign the subscription as contemplated by this section, the Contractor will provide such a code, key, or similar item to the Subscriber at any time and without a fee or charge. A later section in this Agreement governs assignment of a Subscriber's subscription to any Service to a successor in interest.

2.3. Contractor Warranties

The Contractor warrants the following:

- It has validly entered into this Agreement and has the legal power to do so.

- The Services will perform materially in accordance with the applicable user guide and the requirements of this Agreement.
- Subject to any limitations specified in the applicable Service Attachment, the functionality of the Services will not be materially decreased during a subscription term.
- It will in connection with the Service use industry standard virus protection software and approaches designed to protect against the transmission of viruses, worms, time bombs, Trojan horses or other harmful or malicious code, files, scripts, agents or programs ("Malicious Code") to a Subscriber.

For any breach of a warranty above, the State's and individual Subscribers' remedies will be as provided in the section of this Agreement dealing with termination.

Contractor represents and warrants that throughout the Term of this Agreement: (i) all Service components, shall interface and be compatible with each other; (ii) the Service shall be capable of delivering all of the functionality set forth in this Agreement; and (iii) the Service will meet the system performance requirements as set forth in the Service Attachment.

EXCEPT AS SPECIFIED IN THIS AGREEMENT, CONTRACTOR MAKES NO WARRANTIES HEREUNDER WITH RESPECT TO THE SERVICE, OR ANY PART THEREOF AND EXPLICITLY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED.

2.4. State and Subscribers Responsibilities

The State and each Subscriber will be responsible for their respective compliance with this Agreement. Additionally, each Subscriber will:

- Be responsible for the accuracy, quality, and legality of its data and of the means by which the data was acquired.
- Use commercially reasonable efforts to prevent unauthorized access to or use of the Services to which it subscribes and notify the Contractor promptly of any unauthorized access or use of which it becomes aware.
- Use the Services only in accordance with this Agreement, the Service Attachment, the applicable user guide, and in connection with any Acceptable Use Policy attached to the Service Attachment, to the extent it is not inconsistent with this Agreement.
- Use industry standard virus protection software and approaches designed to protect against the transmission of Malicious Code to the Service.

A Subscriber may not:

- Make the Services available to anyone other than its employees and contractors acting on its behalf.
- Decompile, reverse engineer or apply any other process or procedure to derive source code thereof,
- Sell, resell, rent or lease the Services,
- Use the Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights.
- Intentionally interfere with or disrupt the integrity or performance of the Services or third-party data contained therein.

- Attempt to gain unauthorized access to the Services or their related systems or networks.
- Use the Services or the output thereof in any way that is (1) fraudulent, misleading, harmful or in violation of applicable law, rule or regulation, or (2) prohibited by this Agreement.

2.5. Generated Files

"Generated Files" are the results of the search queries that a Subscriber runs using the uFACTS application. Such Generated Files are not included in the definition of "Subscriber's Data" in a later section of this Agreement because they are not stored within the Service; instead, Subscribers must make and retain copies of the Generated Files they produce as a result of using the Service. As between the Subscriber and the Contractor, the Subscriber will own all Generated Files that the Subscriber receives by using the uFACTS application. In the Subscriber's distribution of the Generated Files, the Subscriber may not use the Contractor's name, logo, or trademarks, except to the extent that such are incorporated in such Generated Files by the design of a Service when used as intended.

3. Insurance, Indemnification, Limitation of Liability

3.1. Insurance

Insurance
Contractor shall procure and maintain for the duration of the contract insurance against claims for injuries to persons or damages to property which may arise from or in connection with the performance of the work hereunder by the Contractor, its agents, representatives, or employees. Contractor shall procure and maintain for the duration of the contract insurance for claims arising out of their services and including, but not limited to loss, damage, theft or other misuse of data, infringement of intellectual property, invasion of privacy and breach of data.

MINIMUM SCOPE AND LIMIT OF INSURANCE

Coverage shall be at least as broad as:

1. Commercial General Liability (CGL): written on an "occurrence" basis, including products and completed operations, property damage, bodily injury and personal & advertising injury with limits no less than $1,000,000 per occurrence. If a general aggregate limit applies, either the general aggregate limit shall apply separately to this project/location or the general aggregate limit shall be twice the required occurrence limit. Defense costs shall be outside the policy limit.
2. Automobile Liability: covering Code 1 (any auto), or if Contractor has no owned autos, Code 8 (hired) and 9 (non-owned), with a limit no less than $1,000,000 per accident for bodily injury and property damage.
3. Workers' Compensation insurance as required by the State of Ohio, or the state in which the work will be performed, with Statutory Limits, and Employer's Liability Insurance with a limit of no less than $1,000,000 per accident for bodily injury, $1,000,000 per employee for bodily injury by disease and $1,000,000 policy limit for bodily injury by disease. If Contractor is a sole proprietor, partnership or has no statutory requirement for workers' compensation, Contractor must provide a letter

stating that it is exempt and agreeing to hold Entity harmless from loss or liability for such.

4. Technology Professional Liability (Errors and Omissions) Insurance appropriate to the Contractor's profession, with limits not less than $2,000,000 per claim, $2,000,000 aggregate for legal liability arising out of or resulting from wrongful acts, errors omissions in negligence in performance of work under this Agreement. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Contractor in this agreement and shall cover Contractor personnel or subcontractors, as applicable, who perform professional services related to this agreement.
5. Cyber liability (first and third party) with limits not less than $2,000,000 per claim, $10,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Contractor in this agreement and shall include, but not be limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The coverage shall provide for breach response costs as well as regulatory fines and penalties and credit monitoring expenses with limits sufficient to respond to these obligations. The Cyber Liability insurance is embedded in Contractor's Technology Professional Liability coverage form.

The Insurance obligations under this agreement shall be the minimum Insurance coverage requirements and/or limits shown in this agreement. Any insurance proceeds in excess of or broader than the minimum required coverage and/or minimum required limits, which are applicable to a given loss, shall be available for such loss. No representation is made that the minimum Insurance requirements of this agreement are sufficient to cover the obligations of the Contractor under this agreement.

The insurance policies are to contain, or be endorsed to contain, the following provisions:

Additional Insured Status
Except for Workers' Compensation and Professional Liability insurance (including Technology Liability and Cyber Liability), the State of Ohio, its officers, officials and employees are to be covered as additional insureds with respect to liability arising out of work performed by or on behalf of the Contractor including materials, parts, or equipment furnished in connection with such work. Coverage can be provided in the form of a blanket endorsement to the Contractor's insurance.

Primary Coverage
For any claims related to this contract, the Contractor's insurance coverage shall be primary insurance. Any insurance or self-insurance maintained by the State of Ohio, its officers, officials and employees shall be excess of the Contractor's insurance and shall not contribute with it.

Umbrella or Excess Insurance Policies
Umbrella or excess commercial liability policies may be used in combination with primary policies to satisfy the limit requirements above. Such Umbrella or excess commercial liability policies shall apply without any gaps in the limits of coverage and be at least as broad as and follow the form of the underlying primary coverage required above.

Notice of Cancellation
Contractor shall provide State of Ohio with 30 days written notice of cancellation or adverse material change to any insurance policy required above, except for non-payment cancellation, unless Contractor is able to obtain replacement insurance meeting all of the requirements and specifications herein without lapse and provides the State with the replacement certifications. Adverse material change shall be defined as any change to the minimum insurance limits, terms or conditions that would limit or alter the State's available recovery under any of the policies required above. A lapse in any required insurance coverage during this Agreement shall be a breach of this Agreement.

Waiver of Subrogation
Contractor hereby grants to State of Ohio a waiver of any right to subrogation which any insurer of said Contractor may acquire against the State of Ohio by virtue of the payment of any loss under such insurance, unless prohibited by law. Contractor agrees to obtain any endorsement that may be necessary to affect this waiver of subrogation, but this provision applies regardless of whether or not the State of Ohio has received a waiver of subrogation endorsement from the insurer.

Deductibles and Self-Insured Retentions
Deductibles and self-insured retentions must be declared to and approved by the State. The State may require the Contractor to provide proof of ability to pay losses and related investigations, claims administration and defense expenses within the retention in the form of a financial stability statement.

Claims Made Policies
If any of the required policies provide coverage on a claims-made basis:
1. The Retroactive Date must be shown and must be before the date of the contract or the beginning of contract work.
2. Insurance must be maintained and evidence of insurance must be provided for at least five (5) years after completion of the contract of work.
3. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a Retroactive Date prior to the contract effective date, the Contractor must purchase "extended reporting" coverage for a minimum of five (5) years after completion of contract work. The Discovery Period must be active during the Extended Reporting Period for wrongful acts committed prior to such cancellation or non-renewal.

Verification of Coverage
Contractor shall furnish the State of Ohio with original industry standard Acord certificates and amendatory endorsements for waiver of subrogation and blanket addition insured effecting coverage required by this clause. All certificates and endorsements are to be received and approved by the State of Ohio before work commences. However, failure to obtain the required documents prior to the work beginning shall not waive the Contractor's obligation to provide them. The State of Ohio reserves the right to require the identified endorsements required by these specifications, at any time.

Subcontractors
Contractor shall require and verify that all subcontractors maintain insurance meeting all the requirements stated herein, and Contractor shall ensure that State of Ohio is an additional insured on applicable insurance required from subcontractors.

Special Risks or Circumstances
State of Ohio reserves the right to modify these requirements with reasonable advance written notice, including limits, based on the nature of the risk, prior experience, insurer, coverage, or other special circumstances.

3.2. Indemnification for Infringement

The Contractor will defend the State and the Subscribers against all third party claims that the Service infringes a patent or copyright or constitutes and unauthorized use of any trade secret of such third party, and will indemnify and hold the State and the Subscribers harmless from and against any damages, liabilities and costs finally awarded by a court or amounts paid in a settlement agreed to by Contractor. Any defense of the State or a State Subscriber requires and is subject to the approval and consent of the Ohio Attorney General. Any such defense will be at the Contractor's sole cost and expense. This obligation of defense and indemnification will not apply (i) where the State or a Subscriber has modified or misused the Service and the claim or the suit is based on the modification or misuse, or (ii) the claim arises out of (A) information, materials, specifications, requirements or data provided by or on behalf of the State or a Subscriber, or (B) use of the Service in combination with any platform, product, or data not provided by Contractor or for which the Service is not designed or intended to be used in conjunction with, where the infringement would not have occurred but for the combination. The State or affected Subscribers will give the Contractor notice of any such claim as soon as reasonably practicable, cooperate with the Contractor in all reasonable respects in connection with the claim, and allow the Contractor to control the defense of any such claim, upon consultation with and the approval of the Office of the State's Attorney General.

If a successful claim of infringement is made, or if the Contractor reasonably believes that an infringement or similar claim that is pending may succeed, the Contractor will do one of the following four things as soon as reasonably possible to avoid or minimize any interruption of the Subscribers business:

1. Modify the offending Service so that it is no longer infringing but provides substantially the same functionality as before the modification.
2. Replace the offending Service with an equivalent or better, non-infringing offering.
3. Acquire the right for the Subscribers to use the infringing Service as it was intended to be used under this Agreement.
4. Terminate the infringing Service and refund a pro-rata portion of the amount the Subscribers paid for the Service.

The foregoing provisions of this Section 3.2 constitutes the sole and exclusive remedy of State and the Subscribers, and the sole and exclusive obligation of Contractor, relating to a claim that the Service infringes any patent, copyright or other intellectual property right of a third party.

3.3. Limitation of Liability

A) The State's and each Subscribers' liability for damages under a Service Attachment, whether in contract, law, or equity, will not exceed $300,000.00; except that the foregoing will not limit amounts owing by State or Subscriber to Contractor for the charges thereunder.

B) The Contractor's, its contractors and their respective personnel will not be responsible for any liability, claims, losses and damages arising out of the performance of this cloud services agreement for an aggregate amount in excess of $300,000.00.

C) NEITHER PARTY, ITS AFFILIATES OR CONTRACTORS WILL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, EXEMPLARY, OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, EVEN IF THE PARTY KNEW OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES.

D) The provisions of this Section 3.3 shall not apply to any damages (i) for which Contractor has an obligation to indemnify the State or a Subscriber under Section 3.2, (ii) to a breach of the restrictions on use of the Service set forth in this Agreement or the Service Attachment, or (iii) to the extent resulting from a party's bad faith or intentional misconduct.

4. Confidentiality and Handling of Data

4.1. Confidentiality

The State may disclose to the Contractor written material or oral or other information that the State treats as confidential ("State Confidential Information"). Title to the State Confidential Information and all related materials and documentation the State delivers to the Contractor will remain with the State. The Contractor must treat such State Confidential Information as secret if it is so marked, otherwise identified as such, or when, by its very nature, it deals with matters that, if generally known, would be damaging to the best interests of the public, other contractors or potential contractors with the State, or individuals or organizations about whom the State keeps information. The Contractor may not disclose any State Confidential Information to third parties without the State's consent, using at least the same degree of care as it employs in maintaining in the confidence its own confidential information of a similar nature, but in no event less than a reasonable degree of care, and must use it solely to perform under this Agreement.

The Service delivered under this Agreement is confidential to Contractor, and any data, documentation, or other written information contained therein or provided in connection therewith that is confidential in nature and properly labeled as such ("Contractor Confidential Information"), will be Confidential Information for purposes of this section. The State will keep all such Contractor Confidential Information in confidence and will not use it other than as authorized under this Agreement. Nor will the State disclose any such Confidential Information to any third party without first obligating the third party to maintain the secrecy of the Confidential Information.

If one Party discloses Confidential Information ("Disclosing Party") to the other Party to this Agreement ("Receiving Party"), the Receiving Party's obligation to maintain the confidentiality of the Confidential Information will not apply where such:

1. was already in the possession of the Receiving Party without an obligation of confidence;
2. is independently developed by the Receiving Party;
3. except as provided in the next paragraph, is or becomes publicly available without a breach of this Agreement;

4. is rightfully received by the Receiving Party from a third party without an obligation of confidence;
5. is disclosed by the Receiving Party with the written consent of the Disclosing Party; or
6. is released under a valid order of a court or governmental agency, provided that the Receiving Party notifies the Disclosing Party of the order immediately upon receipt of it, unless it is legally prohibited from doing so.

Information that may be available publicly through other sources about people that is personal in nature, such as medical records, addresses, phone numbers, social security numbers, and similar things, is nevertheless sensitive in nature and may not be disclosed or used in any manner except as expressly authorized in this Agreement. Therefore, item (iii) in the preceding paragraph does not apply, and the Contractor must treat such information as Confidential Information whether it is available elsewhere or not.

The Receiving Party must return all originals of any Confidential Information and destroy any copies it has made on termination or expiration of this Agreement; except as necessary to evidence its performance hereunder provided that any such retained copies shall remain subject to the confidentiality obligations herein.

The disclosure of the Confidential Information of the Disclosing Party in a manner inconsistent with the terms of this provision may cause the Disclosing Party irreparable damage for which remedies other than injunctive relief may be inadequate, and each Receiving Party agrees that in the event of a breach of the Receiving Party's obligations hereunder, the Disclosing Party will be entitled to seek temporary and permanent injunctive relief to enforce the provisions of this Agreement without the necessity of proving actual damages. However, this provision does not diminish or alter any right to claim and recover damages.

This Agreement is not Confidential Information. All its terms and conditions, including pricing and any attachments, represent public information.

4.2. Public Records Requests.

Should the Contractor receive any public records request with respect to any Subscriber's Data, the Contractor will immediately notify any affected Subscriber and fully cooperate with the affected the Subscriber directs.

4.3. Handling of Subscriber's Data

"Subscriber's Data" is any information, data, files, or software of the Subscriber that a Subscriber uses or stores on or in conjunction with the Service. The parties acknowledge and agree that the Service does not involve storing, using, or transmitting Subscriber's Data.

5. Requesting Service

5.1. Acceptance

The acceptance procedure for setup or installation of a Service is governed by the terms of the Contract and can be found in the agreed to uFACTS SOW General Terms and Conditions.

5.2. Service

The Contractor must act as the sole point of contact for all Services under this Agreement and any related Service Attachments for all Subscribers. The Contractor may not require a Subscriber to contact any of the Contractor's third-party suppliers or otherwise transact business directly with such suppliers for any Services ordered under this Agreement, and in all respects, the Contractor must maintain a seamless, single-point-of-contact business relationship with each Subscriber for the Services ordered under this Agreement.

6. Termination – Agreement, Service Attachments, Orders

6.1. Termination by the State

The Contractor must comply with all terms and conditions of this Agreement. If the Contractor is in material breach of its obligations under this Agreement, it will be in default, and the State may proceed in any or all the following ways:

1. The State may terminate this Agreement or the affected Order(s) under this Agreement upon 30 days written notice to Contractor with an opportunity for Contractor to cure the breach within such notice period.
2. The State may file a complaint for damages with a court of competent jurisdiction in Ohio.

The State also may terminate this Agreement or an Order for its convenience with 30 days written notice to the Contractor. In any such event, each Subscriber must pay for all accrued and unpaid charges for Services and any fee specified in the affected Service Attachment(s) for early termination ("Early Termination Charge"), if applicable.

The State's funds are contingent upon the availability of lawful appropriations by the Ohio General Assembly. If the General Assembly fails at any time to continue funding for the payments and other obligations due as part of this Agreement, the State's obligations under this Agreement to pay for amounts incurred after the date the funding expires will terminate and State will have no obligation to pay any Early Termination Charge outlined in any affected Service Attachment(s). The State will not place any orders after the expiration of such funding.

6.2. Termination of Orders by Subscriber or Contractor

Under this Agreement, specific Orders also may be terminated by either a Subscriber or the Contractor, as follows:

6.2.1. By a Subscriber

A Subscriber may terminate Service it has placed under a service attachment, and it may do so at any time for any or no reason upon written notice to Contractor. The Subscriber

will be liable for the Service charges due but unpaid as of the termination date, as well as any Early Termination Charge outlined in the Service Attachment. Where amounts payable under the Service Attachment are paid on an annual basis, no early termination under this clause will entitle Subscriber to a refund of any such yearly amounts paid or payable.

If the Subscriber's funds are contingent upon the availability of lawful appropriations by the Ohio General Assembly or other governmental body, and the General Assembly or other governmental body fails at any time to continue funding for the payments and other obligations due under an Order, the Subscriber's obligations with respect to that Order to pay for amounts incurred after the date the funding expires will terminate, and the Subscriber will have no obligation to pay any Early Termination Charge outlined in any affected Service Attachments. Subscriber will not place any orders after expiration of such funding.

6.2.2. By the Contractor

If a Subscriber materially defaults in the performance of any of its duties or obligations under this Agreement, the Contractor, by giving at least 30 days prior written notice, may cancel any affected Services provided to that Subscriber under this Agreement.

If the Subscriber cures the default before the cancellation of Service date, the Order or Agreement will remain in full force and effect.

If the Subscriber fails to cure, then the Subscriber will remain liable for charges accrued but unpaid as of the cancellation date and any Early Termination Charge as outlined in the appropriate Service Attachment(s), if applicable.

7. Financial – Fees, Claims and Disputes, Billing, and Payment

7.1. Fees

All applicable charges are fully documented in the Service Attachment. The Subscriber will not be responsible for any charges not documented in the Service Attachment or be responsible for any charges waived by the Contractor in this Agreement or the Service Attachment.

Fees are subject to increases as set forth in the Service Attachment.

Subscribers are not responsible for any charges from the Contractor's third-party suppliers for any Services ordered under this Agreement, unless an applicable Service Attachment expressly provides otherwise. In this regard, the Contractor is the seller or reseller of all Services covered by this Agreement, and any payments due to the Contractor's third-party suppliers for Services under this Agreement are included in the Contractor's fees specified in the applicable Service Attachment, unless that Service Attachment expressly provides otherwise.

7.2. Billing

Unless otherwise agreed, invoices will be issued at the Order level, but the Subscriber may require a recap at the agency, division, or district level based on the organizational structure of the Subscriber.

Invoices must be submitted to the State according to the designated "bill to address". The invoice must be submitted within 60 days of the Service. If the Subscriber does not receive the invoice within the 60 days of the date of Service, the Subscriber will be entitled to deny payment of the invoice.

A proper invoice must include the following information:

1. Name and address of the Contractor as designated in this Agreement.
2. Federal Tax Identification Number of the Contractor as designated in this Agreement.
3. Invoice remittance address as designated in the Agreement.
4. A sufficient description of the Services to allow the Subscriber to identify the Services and perform an audit of the Services.

7.3. Payment

Unless otherwise agreed, payments for Services under this Agreement will be due on the 30th calendar day after the actual receipt of a proper invoice in the office designated to receive the invoice. The Contractor agrees to receive payment from approved vouchers by electronic fund transfer (“EFT”) for Subscribers that rely on them to make payment. The Contractor will cooperate with Subscribers in providing the necessary information to implement EFT. The date the EFT is issued in payment will be considered the date payment is made, or if a Subscriber does not use an EFT process, the date its check or warrant is issued in payment will be considered the date payment is made.

7.4. State Reporting Requirements

The Contractor must provide the State with a recap of all Services provided to the Subscribers on a monthly basis. Additional, specific reporting data requirements may be outlined in the Service Attachment(s).

7.5. Service Level Guarantee and Credits

The Contractor will issue a credit allowance to any Subscriber affected by a Service outage, as defined in the Service Level Agreement contained in the applicable Service Attachment. The credit will appear on the affected Subscriber’s next invoice, or if the Subscriber so requests, the Contractor will issue a check to the Subscriber as payment within 30 days of the request.

8. Support and Adjustments

8.1. Service Support Generally

During the term of the Agreement, the Contractor will provide the Subscriber with support and maintenance as set forth in the Service Attachment. As part of the support the Contractor provides in exchange for the applicable fee, the Contractor also will keep all software current by installing all relevant service packs and patches as well as all updates

and new releases and versions of the software as soon as reasonably possible. The Contractor also will keep its own software offering compatible with any updated third-party software that is part of the Services or supports the Services. The way the Contractor provides support will be governed by the Contractor's policies and programs described in the applicable documentation or other materials that the Contractor uses to notify its customers generally of such policies. But regardless of the Contractor's policies and programs, unless otherwise agreed in the applicable Service Attachment, in all cases such support must comply with the requirements of this Agreement and the applicable Service Attachment(s). And the Contractor must provide the support in a competent, professional, and timely manner.

8.2. Updates, Modifications and Enhancements

Except for the support and maintenance to be provided by Contractor as specifically set forth in the Service Attachment, Contractor shall have no obligation under this Agreement to provide updates, modifications or enhancements to the Service, or to provide maintenance, support or other services with respect to the Service. Any updates, modifications or enhancements provided to State or a Subscriber as part of the support and maintenance or otherwise shall be and remain the sole and exclusive property of Contractor and the term "Service" or "Services" as used herein shall include such updates, modifications or enhancements.

8.3. Adjustments

A Subscriber may acquire subscriptions that are based on the number of users, nodes, computers, processors, or other counts of items covered by an Order ("Objects"). In any such cases, the Subscriber may request the fees for a subscription renewal be calculated based on fewer Objects than included in the previous Order, with an appropriate adjustment in the applicable fee(s). For any reduction, fees for the remaining Objects will be as specified in the applicable tier in the Service Attachment.

During a Service Attachment's or an Order's duration ("Order Term"), a Subscriber may increase the volume of its Order (e.g., add additional users) without increasing the Order Term. The cost of any addition Objects or similar increase in usage must be prorated to reflect the time remaining in the Order Term rather than be based on the full Order Term.

8.4. Support Parameters

A Subscriber may initiate support requests for problems it encounters with the Service as set forth in the Service Attachment.

9. Standard Provisions

9.1. Certification of Funds

None of the rights, duties, or obligations in this Agreement will be binding on the State or a Subscriber, and the Contractor will not begin its performance, until all the following conditions occur for that Order:

1. All statutory provisions under the ORC, including Section 126.07, have been met.
2. All necessary funds are made available by the appropriate State agencies.

3. If required, approval of this Agreement or the applicable Order is given by the Controlling Board of Ohio.
4. If the Subscriber is relying on federal or third-party funds for its Order, the Subscriber gives the Contractor written notice that such funds have been made available.

9.2. Excusable Delay

Neither Party will be liable for any delay in its performance arising from causes beyond its control and without its negligence or fault. The delayed Party will notify the other promptly of any material delay in performance and will specify in writing the proposed revised performance date or dates as soon as practicable after notice of delay. The proposed date or dates must be reasonable and cannot exceed the actual delay caused by the events beyond the control of the Party. In the case of such an excusable delay, the dates of performance or delivery affected by the delay will be extended for a period equal to the time lost by reason of the excusable delay. The delayed Party must also describe the cause of the delay and what steps it is taking to remove the cause.

The delayed Party may not rely on a claim of excusable delay to avoid liability for a delay if the delayed Party has not taken commercially reasonable steps to mitigate or avoid the delay. Things that are controllable by the Contractor's suppliers will be considered controllable by the Contractor.

In the case of subscriptions to Services for a term that an excusable delay interrupts, the term of that subscription will be extended at no additional cost to affected Subscribers by the same amount of time as the excusable delay.

9.3. Employment Taxes

Each Party will be solely responsible for reporting, withholding, and paying all employment related taxes, contributions, and withholdings for its own personnel, including, but not limited to, federal, state, and local income taxes, and social security, unemployment and disability deductions, withholdings, and contributions, together with any interest and penalties.

9.4. Sales, Use, Excise, and Property Taxes

The State and most Subscribers are exempt from any sales, use, excise, and property tax. To the extent sales, use, excise, or any similar tax is imposed on the Contractor in connection with any Service, such will be the sole and exclusive responsibility of the Contractor, and the Contractor will pay such taxes (together with any interest and penalties not disputed with the appropriate taxing authority) whether they are imposed at the time the Services are rendered or a later time.

9.5. Equal Employment Opportunity

The Contractor will comply with all state and federal laws regarding equal employment opportunity and fair labor and employment practices, including ORC Section 125.111 and all related Executive Orders.

Before this Agreement can be awarded or renewed, an Affirmative Action Program Verification Form must be submitted to the DAS Equal Opportunity Division to comply with the affirmative action requirements. Affirmative Action Verification Forms and approved Affirmative Action Plans can be found by to the Ohio Business Gateway at:

http://business.ohio.gov/efiling/

The State encourages the Contractor to purchase goods and services from Minority Business Enterprises ("MBEs") and Encouraging Diversity, Growth and Equity ("EDGE") contractors.

9.6. Drug-Free Workplace

The Contractor must comply with all applicable state and federal laws regarding keeping a drug-free workplace. The Contractor must make a good faith effort to ensure that all its employees, while working on State property or the property of any Subscriber, will not have or be under the influence of illegal drugs or alcohol or abuse prescription drugs in any way.

9.7. Conflicts of Interest

No Contractor personnel may voluntarily acquire any personal interest that conflicts with the Contractor's responsibilities under this Agreement. Additionally, the Contractor will not knowingly permit any public official or public employee who has any responsibilities related to this Agreement to acquire an interest in anything or any entity under the Contractor's control, if such an interest would conflict with that official's or employee's duties. The Contractor will disclose to the State knowledge of any such person who acquires an incompatible or conflicting personal interest related to this Agreement. The Contractor will take all legal steps to ensure that such a person does not participate in any action affecting the work under this Agreement, unless the State has determined that, in the light of the personal interest disclosed, that person's participation in any such action would not be contrary to the public interest.

9.8. Assignment

Neither party may assign this Agreement or any of its rights or obligations under this Agreement without the prior, written consent of the other party.

9.9. Governing Law

This Agreement will be governed by the laws of Ohio, and venue for any disputes will lie with the appropriate court in Ohio.

9.10. Finding for Recovery

The Contractor warrants that the Contractor is not subject to an unresolved finding for recovery under ORC §9.24. If the warranty is false on the date the Parties signed this Agreement, the Agreement is void *ab initio*.

9.11. Publicity and Branding

The Contractor must not do the following without prior, written consent from the State:

1. Advertise or publicize that the Contractor is doing business with the State;
2. Use this Contract as a marketing or sales tool; or
3. Affix any advertisement or endorsement, including any logo, graphic, text, sound, video, and company name, to any State-owned property, application, or website, including any website hosted by Contractor or a third party.

9.12. Prohibition of the Expenditure of Public Funds for Offshore Services

No State Cabinet, Agency, Board or Commission will enter into any contract to purchase services provided outside the United States or that allows State data to be sent, taken, accessed, tested, maintained, backed-up, stored, or made available remotely outside (located) of the United States. Notwithstanding any other terms of this Contract, the State reserves the right to recover any funds paid for services the Contractor performs outside of the United States for which it did not receive a waiver. The State does not waive any other rights and remedies provided the State in the Contract.

The Contractor must complete the Contractor/Subcontractor Affirmation and Disclosure form affirming the Contractor understands and will meet the requirements of the above prohibition. During the performance of this Contract, the Contractor must not change the location(s) disclosed on the Affirmation and Disclosure Form, unless a duly signed waiver from the State has been attained to perform the services outside the United States.

9.13. Campaign Contributions

By signing this document, the Contractor certifies that all applicable parties listed in ORC Section 3517.13 are in full compliance with ORC Section 3517.13.

9.14. Export Compliance

The Services and derivatives thereof may be subject to export laws and regulations of the United States and other jurisdictions. Both the Contractor and the State represent that it is not named on any U.S. government denied-party list. Neither Party will permit others to access or use the Services in a US-embargoed country or in violation of any U.S. export law or regulation.

9.15. Safety and Security Rules

When on any property owned or controlled by the State or Subscribers, the Contractor must comply with all security and safety rules applicable to people on those premises.

9.16. Ohio Ethics Law

The Contractor certifies that it is currently in compliance with and will continue to adhere to the requirements of the Ohio ethics laws. The Contractor also certifies that all applicable parties listed in Ohio Revised Code Section 3517.13 are in full compliance with that section.

9.17. Entire Agreement

This Agreement, together with the Service Attachment and all additional documents expressly incorporated herein, sets forth the entire agreement of the Parties with respect to the subject matter hereof and supersedes any prior agreements, promises, representations, understandings, and negotiations between the Parties with respect to the subject matter hereof.

Further, neither the Subscriber nor the Contractor may add or require additional terms as part of any authorized Order or Service Attachment unless there is written agreement by the Parties to do so. Documents attached to a Service Attachment as exhibits to be executed by a Subscriber typically identify authorized Service options the Subscriber has selected, provide information about a Subscriber, identify installation or configuration requirements or similar statements of work to be done by the Contractor, set schedules for performance, and similar matters.

9.18. Severability

If any provision hereunder is held invalid, illegal, or unenforceable by a court of competent jurisdiction, this Agreement will be revised only to the extent necessary to make that provision legal and enforceable or, if that is not possible, the unaffected portions of this Agreement will remain in full force and effect so long as the Agreement remains consistent with the Parties' original intent.

9.19. Survival

Any terms or conditions contained in this Agreement that must survive termination or expiration of this Agreement to be fully effective will survive the termination or expiration of the Agreement, unless expressly provided otherwise in this Agreement. Additionally, no termination or expiration of the Agreement will affect the State's right to receive Services, and its obligations with respect to such Services, for which the State has paid before expiration or termination, but no subscription to a Service will continue beyond the period paid for before termination or expiration of the Agreement.

9.20. No Waiver

The failure of a Party to demand strict performance of any terms or conditions of this Agreement may not be construed as a waiver of those terms or conditions, and that Party may later demand strict and complete performance by the other Party.

9.21. Order of Precedence

If a conflict between the terms and conditions of this Master Services Agreement and those in a Service Attachment arises, this Master Services Agreement will prevail, unless the Service Attachment specifically provides otherwise. If a user guide or other documentation is incorporated into the Agreement by reference, this Agreement, including any applicable Service Attachment(s), will prevail over any conflicting terms or conditions in any such incorporated documentation.

9.22. Headings

The headings herein are for convenience only and are not intended to have any substantive significance in interpreting this Agreement.

9.23. Governmental Authorization, Regulatory Changes

Each party must comply with all applicable federal, state, and local laws, rules, orders, and regulations in performing its obligations hereunder. To the extent any provision of this Agreement conflicts with any such law, rule, order, or regulation, that law, rule, order, or regulation will supersede the conflicting provision of this Agreement.

The Contractor may discontinue, limit, or impose additional requirements to the provision of Service, upon no less than 30 days written notice, if required to meet federal, state or local laws, rules, orders, or regulations. But if any such action materially affects any Subscriber's use of a Service, the Subscriber may on written notice to the Contractor terminate its use of the Service without an Early Termination Charge and receive a pro rata refund of any amounts paid in advance for the Service.

9.24. Notices

Except as otherwise provided in this Agreement, all notices hereunder must be in writing and may only be sent by registered or certified mail, postage prepaid; facsimile transmission, overnight courier, or email, upon confirmation of receipt.

Alternatively, such notices may be hand delivered if confirmation of receipt is attained at delivery.

The State's address for notification is:

Department of Job and Family Services
Contracts and Acquisitions
30 East Broad Street
Columbus, Ohio 43215
Attention: Deputy Director

The Contractor's address for notification is:

Deloitte Consulting LLP
180 East Broad Street Ste 1400
Columbus, OHI 43215
Attn: David Doyle

9.25. Amendments

No amendment or modification of this Agreement will be effective unless it is in writing and signed by both Parties.

9.26. Boycotting

Pursuant to Ohio Revised Code 9.76 (B) Contractor warrants that Contractor is not boycotting any jurisdiction with whom the State of Ohio can enjoy open trade, including Israel, and will not do so during the contract period.

9.27. Registration with the Secretary of State.

By providing a Charter Number and signature within the Certification Offer Letter, the Contractor attests that the Contractor is:

A foreign corporation, not incorporated under the laws of the state of Ohio, but is registered with the Ohio Secretary of State pursuant to Ohio Revised Code Sections 1703.01 to 1703.31, as applicable.

Any foreign corporation required to be licensed under O.R.C. § 1703.01-1703.31, which transacts business in the state of Ohio, without being so licensed, or when its license has expired or been canceled, shall forfeit not less than $250.00 nor more than ten thousand dollars. No officer of a foreign corporation (http://codes.ohio.gov/orc/1703.01) shall transact business in the state of Ohio, if such corporation is required by O.R.C. § 1703.01-1803.31 to procure and maintain a license, but has not done so. Whoever violates this is guilty of a misdemeanor of the fourth degree. Questions regarding registration should be directed to (614) 466-3910, or visit http://www.sos.state.oh.us

TO SHOW THEIR AGREEMENT, the Parties have executed this Agreement on the date(s) identified below.

DELOITTE CONSULTING LLP	**STATE OF OHIO, JOB AND FAMILY SERVICES**
Signature	Signature
Printed Name	Kimberly L. Hall, Director
Title	Title
Date	Effective Date

AFFIRMATION AND DISCLOSURE FORM

By the signature affixed hereto, the Contractor affirms and understands that if awarded a contract, both the Contractor and any of its subcontractors shall perform no services requested under this Contract outside of the United States, nor allow State data to be sent, taken, accessed, tested, maintained, backed-up, stored or made available remotely (located) outside of the United States.

The Contractor shall provide all the name(s) and location(s) where services under this Contract will be performed and where data is located in the spaces provided below or by attachment. Failure to provide this information may result in no award. If the Contractor will not be using subcontractors, indicate "Not Applicable" in the appropriate spaces.

1. Principal location of business of Contractor:

   180 East Broad Street Suite 1400 (Address)
   Columbus, OH 43215 (City, State, Zip)

   Name/Principal location of business of subcontractor(s):

   Not Applicable (Name)
   _____ (Address, City, State, Zip)

   _____ (Name)
   _____ (Address, City, State, Zip)

2. Location where services will be performed by Contractor:

   Gilbert, AZ; Mumbai, India; Hyderabad, India (Address)
   _____ (City, State, Zip)

   Name/Location where services will be performed by subcontractor(s):

   Not Applicable (Name)
   _____ (Address, City, State, Zip)

   _____ (Name)
   _____ (Address, City, State, Zip)

3. Location where state data will be located, by Contractor:

   [redacted] (Address)
   _____ (Address, City, State, Zip)

Name/Location(s) where state data will be located by subcontractor(s):

Not Applicable	
(Name)	(Address, City, State, Zip)
(Name)	(Address, City, State, Zip)

Contractor also affirms, understands and agrees that Contractor and its subcontractors are under a duty to disclose to the State any change or shift in location of services performed by Contractor or its subcontractors before, during and after execution of any Contract with the State. Contractor agrees it shall so notify the State immediately of any such change or shift in location of its services. The State has the right to immediately terminate the contract, unless a duly signed waiver from the State has been attained by the Contractor to perform the services outside the United States.

On behalf of the Contractor, I acknowledge that I am duly authorized to execute this Affirmation and Disclosure Form and have read and understand that this form is a part of any Contract that Contractor may enter into with the State and is incorporated therein.

By: **Deloitte Consulting LLP**
(Contractor)

Print Name: _____

Title: _____

Date: _____

Service Attachment 1

Cloud Service Agreement for uFACTS for PUA/DUA

This Service Attachment (the "Service Attachment") is between Deloitte Consulting LLP ("Contractor"), having an office at 180 East Broad Street Suite 1400, Columbus, OH 43215, and the State of Ohio, through the Department of Job and Family Services ("State"), having its principal place of business at 30 East Broad Street, 32th Floor, Columbus, OH 43215. The State and the Contractor are sometimes referred to jointly as the "Parties" or individually as a "Party". This Service Attachment and its Schedule 1 attached hereto is incorporated into and made a part of the Agreement as is effective as of the effective date of the Agreement.

The State or a State Entity entering into an Order or this Service Attachment (a "Subscriber") for a license to use Contractor's SaaS cloud solution uFACTS for PUA/DUA (the "Service").

1. Definitions.

The defined terms in the CSA will have the same meanings in this Service Attachment as they do in the CSA. There may be additional definitions contained herein.

2. Services.

License.

Subject to a Subscriber's payment to the Contractor of the fees set forth herein or in the uFACTS for PUA/DUA SOW, the Contractor grants the Subscriber on the terms and conditions set forth in this Service Attachment and the Agreement, a limited, non-exclusive and non-transferable license to use the Service solely for the Subscriber's governmental purposes for PUA/DUA. The foregoing license is subject to the additional license restrictions set forth herein and in the Agreement.

Unless agreed to otherwise, the license shall become perpetual as to Contractor's uFACTS for PUA/DUA SOW General Terms and Conditions in accordance with the agreed to uFACTS for PUA/DUA SOW. For clarification, the foregoing perpetual license is not to the Service or as defined above third party SaaS cloud platform.

The Service may run on platforms or include software made available by one or more third parties ("Third Party Software") and may include third party data from publicly available databases ("Third Party Data"). All Third-Party Data is provided on an "as is" basis and Contractor shall have no liability for the accuracy of such Third-Party Data.

To the extent any Service provided to Subscriber hereunder constitutes inventory within the meaning of section 471 of the Internal Revenue Code, such Service is licensed to Subscriber by Contractor as agent for its product company subsidiary, Deloitte Consulting Product Services LLC, on the terms and conditions contained in this Agreement.

Standard Service Features. uFACTS for PUA/DUA provides the following high-level features:

- PUA/DUA Program Setup.
- Initial Screening.
- Initial Claim.
- Monetary Determination.

- Certifications.
- Payments.
- Adjudication.
- Accounting.
- Workflow.

These features are described in greater detail within the uFACTS for PUA/DUA SOW.

Provision of Services. The Contractor will make the Services available to the Subscriber pursuant to the Agreement, including this Service Attachment, during the Term hereof, and defined in the uFACTS for PUA/DUA SOW. The State agrees that purchases hereunder are neither contingent on the delivery of any future functionality or features nor dependent on any oral or written public comments made by the Contractor regarding future functionality or features.

The Contractor Responsibilities. The Contractor must provide support for the Services to the Subscribers as described herein and in the uFACTS for PUA/DUA SOW.

State Responsibilities.

State will comply with the Acceptable Use Policy attached hereto as Schedule 1.

3. Fees and Payment

Fee Structure.

Fees. The State and Contractor agree to the fees expressed as the Total Price in the uFACTS PUA/DUA SOW. The fees for the uFACTS Service have been incorporated within the fees for Adaption and Implementation services.

After 90 days, the Contractor may suspend the Services until all delinquent amounts are paid, notwithstanding the prohibition against self-help provided for elsewhere in the Agreement, but the Contractor may not do so if the Subscriber is disputing the applicable charges reasonably and in good faith and is cooperating diligently to resolve the dispute.

Invoicing and Payment. The State and Contractor agree to Invoicing and Payment provisions as described in the uFACTS PUA/DUA General Terms and Conditions.

4. Proprietary Rights

Reservation of Rights in Services. The Service embodies valuable copyright, patent, trademark, trade secret and other intellectual property rights owned or licensed by the Contractor and the Contractor and its licensors retain all right, title and interest in all such proprietary rights and property. Subject to the limited rights expressly granted in Section 2 (License) above, the Contractor and its licensors reserve all rights, title, and interest in and to the Service, including all related intellectual property rights. No rights are granted to the State or Subscribers hereunder other than as expressly set forth herein or elsewhere in the Agreement.

Restrictions. In addition to the restrictions set forth in the Agreement, Subscribers will not intentionally permit any third party to access the Services, except as permitted herein or in the uFACTS PUA/DUA SOW, create derivative works based on the Services except as permitted in the Agreement, reverse engineer the Services, or access the Services to build a competitive product or service or to copy any features, functions, or graphics of the Services. Nothing herein prohibits a Subscriber from porting and hosting Generated Files, as defined in this Agreement, to other sites to support its own business purposes during and after any term of the Agreement.

Subscriber Responsibilities. The Services is solely for the Subscriber's governmental purposes and is not intended by be relied upon by any person or entity other than the Subscriber. The Subscriber shall be responsible for the performance of its personnel and agents and maintaining all software, hardware and other equipment used by the Subscriber to access and use the Service. The Service is available only for the number of authorized users of the Subscriber as described in the applicable Order or Service Attachment ("Users"). The Subscriber will not permit any User ID or User login to be used by more than one individual. The Subscriber is responsible for all activities conducted under its Users' logins and for Users' compliance with this Attachment and the Agreement. Subscriber is responsible for maintaining the security of its account and passwords to prevent and restrict the access and use of the Service from unauthorized individuals.

5. Support and Maintenance Scope

The Contractor must manage, operate, maintain and provide on-going support of the Service, as implemented and deployed by the Contractor, during the term of the Contract.
The Contractor will provide the following break/fix support for the Service:

- Track, monitor and provide remediation for in scope Service defects and issues;
- Identify any defects or issues being resolved for other Contractor clients;
- Identify and implement required system or configuration changes to address Service defects;
- Maintain Service documentation (technical specifications and testing documentation) as well as a compendium of common problems, root causes and remedy to aid in the identification and remediation of underlying system issues;
- Test changes to confirm resolution of defects;
- Identify, specify and system test as applicable third Party supplied patches and fixes for third Party supplied packaged systems software (including OS, BIOS, microcode, patches, service packs and similar), as well as new releases.

For the Services, inclusive of all performance, technical and functional aspects, the Contractor must:

- Maintain the performance, availability and stability of the Service as set forth herein. The Contractor must schedule its implementation of changes so as not to unreasonably interrupt State business operations.

The Contractor must:

- Establish and maintain an emergency notification process to notify key State staff of pending problem areas, for example virus or malware infection, to escalate problems.
- Provide a periodic status notification to the State for service outages and reasonable notification of upcoming releases.
- The Contractor must provide ongoing administration support required to manage software updates, patches and data management for the Service.
- End user manuals, internal procedure manuals, and operating procedures manuals will be updated by the Contractor at a minimum prior to every major release of the Service.

5.1 Contractor Service Desk Support

The Contractor will be required to provide Tier 1, 2 and 3 Service Desk support on state business days from 8:00 a.m. to 5:00 p.m. Columbus, OH local time, excluding State holidays, that will serve as a resource for the State regarding procedures and system issues. The Contractor must staff for Tier 1, 2 and 3 support throughout the day with the number of staff appropriate to meet the requirements and performance specifications defined in Section 6, Service Level Agreements. The Contractor Service Desk Support staff can be contacted at a designated email address and phone number as provided in the Service or as otherwise provided by Contractor. In addition, Contractor will provide Service Desk responsibilities as defined in the uFACTS PUA/DUA SOW.

5.2 Tier 1, 2 and 3 Service Desk Activity Reports

The Contractor must provide monthly reporting on Service Desk activities. Reports must include performance statistics agreed between the parties.

The following tasks are to be, at a minimum, performed by responsible parties in this phase:

Key Tasks	State	Contractor
Document data issues and provide to Subscriber for resolution as applicable.	Support	Perform
Compile and maintain Service issue lists.	Support	Perform
Conduct quality and progress reviews with appropriate Subscriber personnel.	Support	Perform
Provide and maintain Tier 1, 2 and 3 Service Desk Support	Support	Perform
Develop, and thereafter maintain and make available to Subscriber, a knowledge base of documentation gathered throughout the subscription term and allow for re-use of such for future subscriptions or upgrades.	Support	Perform

6. Service Levels

This section sets forth the performance specifications for the Service Level Agreements (SLA) for the Service. The Contractor will be assessed for each SLA failure and the "Service Credit" shall not exceed the monthly Fee at Risk for that period. The Service Credit is the amount due to the Subscriber for the failure of SLAs. For SLAs measured on a quarterly basis, the monthly fee at risk applies and is cumulative.

The Contractor agrees that 10% of the monthly Fee at Risk for the Agreement will be at risk ("Fee at Risk"). The monthly Fee at Risk will be calculated as follows:

((Total Hypercare and M&O fee of the Agreement / 7) x 10 % = Monthly Fee at Risk for the Agreement.

On a quarterly basis, there will be a "true-up" at which time the total amount of the Service Credit will be calculated (the "Net Amount"), and such Net Amount may be off set against any fees owed by the Subscriber to the Contractor, unless the Subscriber requests a payment in the amount of the Service Credit.

The Contractor will not be liable for any failed SLA caused by circumstances beyond its control, and that could not be avoided or mitigated through the exercise of prudence and ordinary care, provided that the Contractor promptly, notifies the Subscriber in writing and takes all steps necessary to minimize the effect of such circumstances and resumes its performance of the Services in accordance with the SLAs as soon as reasonably possible.

To further clarify, the Service Credits available to the Subscriber will not constitute the Subscriber's exclusive remedy to resolving issues related to the Contractor's performance, but any Service Credits paid by Contractor will be applied to offset any damages that Subscriber may seek hereunder for a Service Level Failure. In addition, if the Contractor fails multiple service levels during a reporting period or demonstrates a pattern of failing a specific service level throughout the SOW, then the Contractor may be required, at the State's discretion, to implement a corrective action plan to address the failed performance.

SLAs will commence when the uFACTS for PUA/DUA is implemented into production.

Escalation for Repetitive Service Level Failures
Although it is the Subscriber's intent to escalate service level failures to the Contractor Account Representative, the Subscriber may decide to escalate to other levels within the Contractor's corporate structure deemed appropriate to resolve repetitive service failures.

Monthly Service Level Report
Monthly following implementation into production, the Contractor must provide a written report (the "Monthly Service Level Report") to the State which includes the following information:

- Identification and description of each failed SLA caused by circumstances beyond the Contractor's control and that could not be avoided or mitigated through the exercise of prudence and ordinary care during the applicable month;
- the Contractor's quantitative performance for each SLA;
- the amount of any monthly performance credit for each SLA;
- the year-to-date total performance credit balance for each SLA and all the SLAs;
- upon State request, a "Root-Cause Analysis" and corrective action plan with respect to any SLA where the Individual SLA was failed during the preceding month; and
- trend or statistical analysis with respect to each SLA as requested by the Subscriber.

The Monthly Service Level Report will be due no later than the tenth (10th) day of the following month.

Failure of the Contractor to meet any SLAs in an applicable Service Attachment will not be considered a breach of this warranty section unless the Subscriber reasonably determines that the failure is persistent or extended in duration.

SLA Name	Performance Evaluated	Non-Conformance Remedy	Frequency of Measurement
System Availability	All Service components are Available to All Subscriber Users for All Business Functions. This Service Level does not apply to the availability of External Source systems made available to the Solution. **Compliance with the System Availability Service Level is required to be equal to or greater than 99% in the reporting month. Excludes scheduled maintenance windows.**	If the System Availability Service Level percentage is not met, then the service credit will be $500.00 per each calendar day that the Service was unavailable below the 99% system availability Service Level. For continued performance deficiency occurrences, the State may impose the initial damage amount and may impose an additional Service Credit up to a 5% reduction of the next scheduled payment. The service credit may be deducted from the next	Reporting Month

SLA Name	Performance Evaluated	Non-Conformance Remedy	Frequency of Measurement
		invoice presented for payment.	
Issue Resolution – Time to Repair (Critical Severity Issues)	Prompt resolution of the Service Critical issues. The Subscriber shall, in consultation with the Contractor, determine the Severity of each issue. Formal declaration of the Severity of each issue will be defined below in the Prioritization: Prioritization: An Issue shall be categorized as a “Critical Severity” as defined in within this document. **Compliance with the Issue Resolution – Time to Repair (Critical Severity Issues) Service Level is required to be resolved <72 hours from the time the Subscriber reports the issue as Critical Severity to the Contractor.**	If the issue is not resolved within the Service Level timeframe, then the service credit will be $500.00 per each calendar day beyond the Service Level timeline until the issue is resolved. For continued performance deficiency occurrences, the State may impose the initial damage amount and may impose an additional Service Credit up to a 5% reduction of the next scheduled payment. The service credit may be deducted from the next invoice presented for payment.	Per Occurrence
Issue Resolution – Mean Time to Repair (High Severity 2 Issues)	Prompt resolution of the Service High Severity issues. The Subscriber shall, in consultation with the Contractor, determine the Severity of each issue. Formal declaration of the Severity of each issue will be defined below in the Prioritization: Prioritization: An Issue shall be categorized as a “High Severity Issue” as defined within this document. **Compliance with the Issue Resolution – Mean Time to Repair (High Severity Issues) Service Level is required to be resolved <**	If the issue is not resolved within the Service Level timeframe, then the service credit will be $500.00 per each calendar day beyond the Service Level timeframe until the issue is resolved. For continued performance deficiency occurrences, the State may impose the initial damage amount and may impose an additional Service Credit up to a 5% reduction of the next scheduled payment. The service credit may be deducted from the next	Per Month

SLA Name	Performance Evaluated	Non-Conformance Remedy	Frequency of Measurement
	72 hours from the time the Subscriber reports the issue as High Severity to the Contractor.	invoice presented for payment.	
Issue Resolution – Mean Time to Repair (Severity 3 Issues)	Prompt resolution of the Service Severity 3 issues. The Subscriber shall, in consultation with the Contractor, determine the Severity of each issue. Formal declaration of the Severity of each issue will be defined below in the Prioritization: Prioritization: An Issue shall be categorized as a "Severity 3 Issue" if the issue is characterized by the following attributes as defined below. **Compliance with the Issue Resolution – Mean Time to Repair (Severity 3 Issues) Service Level is required to be resolved < 72 hours from the time the Subscriber reports the issue as Severity 3 to the Contractor.**	If the issue is not resolved within the Service Level timeframe, then the service credit will be $500.00 per each calendar day beyond the Service Level timeline until the issue is resolved. For continued performance deficiency occurrences, the State may impose the initial damage amount and may impose an additional Service Credit up to a 5% reduction of the next scheduled payment. The service credit may be deducted from the next invoice presented for payment.	Per Month
Customer Service Help Desk - Availability	The percentage of time that the Customer Service Help Desk is available for normal business operations. The Contractor must maintain a Customer Service Help Desk in good operating condition so that standard/normal organization activities can take place within defined time frames. **Compliance with the Customer Service Help Desk - Availability Service Level is 98% based on the reporting month.**	If the Customer Service Help Desk - Availability Service Level percentage is not met, then the service credit will be $500.00. For continued performance deficiency occurrences, the State may impose the initial damage amount and may impose an additional Service Credit up to a 5% reduction of the next scheduled payment. The service credit may be deducted from the next invoice presented for payment.	Per Month

The severity levels are defined as follows:

Severity 1 Defects: Severity 1 Defects are those that render the entire system inaccessible to all users or when major features of the system such as batch processing is non-functional.

Severity 2 Defects: Severity 2 Defects are those that impact functionality that impacts majority of the users or critical data but does not have a workaround.

Severity 3 Defects: Severity 3 Defects affect a smaller number of users and has a temporary workaround.

6.1 Escalation Process

Any support call that is not resolved within the timeframe set forth in the SLA matrix above must be escalated within the time periods set forth below after the completion of the SLA timeframe: to the Contractor's management under the following parameters. Unresolved problems that are classified as critical must be escalated to the Contractor's Project Partner, Principal, Managing Director (PPMD) within one hour and to Contractor's Product Owner after four hours. If a Critical Issue is not resolved within one day following the SLA timeframe, it must escalate to the Contractor's Lead Client Service PPMD after two days.

6.2 Subscriber Obligations

To facilitate the Contractor meeting its support obligations, Subscribers must provide the Contractor with the information reasonably necessary to determine the proper classification of the underlying problem. They also must assist the Contractor as reasonably necessary for the Contractor's support personnel to isolate and diagnose the source of the problem. Additionally, to assist the Contractor's tracking of support calls and the resolution of support issues, Subscribers must make a reasonable effort to use any ticket or incident number that the Contractor assigns to a particular incident in each communication with the Contractor.

6.3 Relationship to Support Level Agreements ("SLA")

The Contractor's support obligations set forth in the Agreement are in addition to the SLAs in this Section of this Service Attachment. Furthermore, the SLAs may provide for credits to the Subscribers even though the Contractor is meeting its support obligations hereunder.

7. Terms and Termination

Term of Subscriptions. Subscriptions commence on the start date specified in the applicable Order Form and continue for the subscription term specified therein, subject to relevant provisions in the Agreement, such as the MCSA's termination and the non-appropriation provisions. Should a Subscriber elect to renew a subscription during the period set forth above, provided this Agreement remains in effect, the renewal will be at the Subscriber's option and will be for the fees set forth in the Fee section above.

In Witness Whereof, the Parties have executed this Service Attachment, which is effective on the date the State's duly authorized representative signs it on behalf of the State, ("Effective Date").

DELOITTE CONSULTING LLP	**STATE OF OHIO, JOB AND FAMILY SERVICES**
Signature	Signature
Printed Name	Printed Name
Title	Title
Date	Effective Date

Schedule 1 to Service Attachment

Acceptable Use Policy

This Acceptable Use Policy ("AUP") describes the prohibited uses of the Service. The examples described in this AUP are not exhaustive. We may modify this AUP at any time by posting a revised version on the site where you access the Licensed Software (the "Site"). By using or accessing the Site, you agree to the latest version of this AUP.

1. Compliance with Laws. You will comply with all applicable laws and regulations when using the Site and will not allow any illegal or improper use of the Site.

2. No Security Violations. You may not use the Site to violate the security or integrity of any network, computer or communications system, software application, or network or computing device (each, a "System"). Prohibited activities include:

- Accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System.
- Monitoring of data or traffic on a System without permission.
- Forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route. The legitimate use of aliases and anonymous remailers is not prohibited by this provision.

3. No Network Abuse. You may not make network connections to any users, hosts, or networks unless you have permission to communicate with them. Prohibited activities include:

- Monitoring or crawling of a System that impairs or disrupts the System being monitored or crawled.
- Inundating a target with communications requests so the target either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective.
- Interfering with the proper functioning of any System, including any deliberate attempt to overload a system by mail bombing, news bombing, broadcast attacks, or flooding techniques.
- Operating network services like open proxies, open mail relays, or open recursive domain name servers.
- Using manual or electronic means to avoid any use limitations placed on a System, such as access and storage restrictions.

4. No Illegal, Harmful, or Offensive Use or Content. You may not use, or encourage, promote, facilitate or instruct others to use, the Site for any illegal, harmful, fraudulent, infringing or offensive use, or to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, fraudulent, infringing or offensive. Prohibited activities or content include:

- Any activities that are illegal, that violate the rights of others, or that may be harmful to others, our operations or reputation, including disseminating, promoting or facilitating child pornography, offering or disseminating fraudulent goods, services, schemes, or promotions, make-money-fast schemes, Ponzi and pyramid schemes, phishing, or pharming.
- Content that infringes or misappropriates the intellectual property or proprietary rights of others.
- Content that is defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable, including content that constitutes child pornography, relates to bestiality, or depicts non-consensual sex acts.

- Content or other computer technology that may damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, including viruses, Trojan horses, worms, time bombs, or cancelbots.

5. No E-Mail or Other Message Abuse. All commercial email promoting goods or services you send using the Site must comply with all applicable laws, rules, regulations, industry codes and similar guidelines. Prohibited activities include:

- Creating or sending hoax emails or chain emails;
- Distributing, publishing, sending, or facilitating the sending of unsolicited mass e-mail or other messages, promotions, advertising, or solicitations (like "spam"), including commercial advertising and informational announcements;
- Harvesting email addresses or collecting replies to messages sent from another internet service provider if those messages violate this AUP or the acceptable use policy of that provider;
- Impersonating someone else without the sender's explicit permission or altering or obscuring message header information.

6. Monitoring and Enforcement. We reserve the right, but do not assume the obligation, to investigate any violation of this AUP or misuse of the Site. We may investigate violations of this AUP or misuse of the Site, or remove, disable access to, or modify any content or resource that violates this AUP or any other agreement we have with you for use of the Site. We may report any activity that we suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Our reporting may include disclosing appropriate customer information. We also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this AUP.

7. Suspension or Termination. If you violate the AUP or authorize or help others to do so, we may suspend or terminate your access to the Site.

8. Reporting of Violations of this AUP. If you become aware of any violation of this AUP, you will immediately notify us and provide us with assistance, as requested, to stop or remedy the violation.